Beiträge zum Transnationalen Wirtschaftsrecht

Markus Heinemann

Mehr(Un)Sicherheit? Datenschutz im transatlantischen Verhältnis

Heft 164

Juni 2019

Mehr(Un)Sicherheit?
Datenschutz im transatlantischen Verhältnis

Untersuchung des rechtlichen Status quo, dessen praktische Implikationen und Probleme sowie möglicher Alternativen für den transatlantischen Datenaustausch

Von

Markus Heinemann

Institut für Wirtschaftsrecht
Forschungsstelle für Transnationales Wirtschaftsrecht
Juristische und Wirtschaftswissenschaftliche Fakultät
der Martin-Luther-Universität Halle-Wittenberg

Markus Heinemann, M.Sc., ist Absolvent des Studiengangs „International Area Studies“ an der Martin-Luther-Universität Halle-Wittenberg und Student des postgraduellen Studiengangs „Master of Business Law and Economic Law“ am Institut für Wirtschaftsrecht der Martin-Luther-Universität Halle-Wittenberg.

Christian Tietje/Gerhard Kraft/Christoph Kumpan (Hrsg), Beiträge zum Transnationalen Wirtschaftsrecht, Heft 164

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://www.dnb.ddb.de abrufbar.

ISSN 1612-1368 (print)
ISSN 1868-1778 (elektr.)

ISBN 978-3-96670-001-6 (print)
ISBN 978-3-96670-002-3 (elektr.)

Schutzgebühr Euro 5

Die Hefte der Schriftenreihe „Beiträge zum Transnationalen Wirtschaftsrecht“ finden sich zum Download auf der Website des Instituts bzw. der Forschungsstelle für Transnationales Wirtschaftsrecht unter den Adressen:

http://institut.wirtschaftsrecht.uni-halle.de/de/node/23
http://telc.jura.uni-halle.de/de/node/23

Institut für Wirtschaftsrecht
Forschungsstelle für Transnationales Wirtschaftsrecht
Juristische und Wirtschaftswissenschaftliche Fakultät
Martin-Luther-Universität Halle-Wittenberg
Universitätsplatz 5
D-06099 Halle (Saale)
Tel.: 0345-55-23149 / -55-23180
Fax: 0345-55-27201
E-Mail: ecohal@jura.uni-halle.de

INHALTSVERZEICHNIS

A. Einleitung

> "Personal data is the currency of today's digital market. And like any currency it needs stability and trust. Only if consumers can 'trust' that their data is well protected, will they continue to entrust businesses and authorities with it, buy online, and accept new services – the new services, you in this audience, invent and develop."[1]

Den Entwurf der neuen Datenschutz-Grundverordnung (DSGVO) vorstellend, unterstrich *Viviane Reding*, die damalige Vizepräsidentin der Europäischen Kommission (EU-KOMM), die Bedeutung von Daten als Währung des Handels im digitalen Zeitalter. Erhebung, Austausch und vor allem die Analyse von Daten jeglicher Art über Staatsgrenzen hinweg sind heute für Unternehmen in der Europäischen Union und den USA systemrelevant. 2016 waren 50 % der transatlantischen Dienstleistungsexporte digitalen Ursprungs, Tendenz steigend.[2] 90 % des Umsatzes von Google und 95 % des Umsatzes von Facebook als kommerzielle Avantgarde der Internetökonomie basieren auf der Analyse von persönlichen Daten und deren Kopplung an Werbung.[3]

Die Nutzung von Daten für kommerzielle und nicht-kommerzielle Ziele birgt enormes Potenzial. Transportkosten können durch autonome Logistiksysteme um ein Viertel gesenkt und Rohstoffe dadurch gespart werden. Krankheitsbilder können durch Kombination und Analyse exorbitanter Datenmengen besser erforscht werden.[4] Allerdings besteht bei nicht reguliertem Austausch von Daten zwischen Unternehmen die Gefahr des Kontrollverlusts für eben diese, deren Kunden und andere Marktakteure.[5]

Für die Funktion und das Gleichgewicht des skizzierten Datenmarktes gelten laut *Viviane Reding* zwei notwendige Bedingungen: Stabilität und Vertrauen. Beide bedingen und beeinflussen sich gegenseitig. Äquivalent zum Dollar oder zum Euro ist der Datenaustausch zwischen den Märkten der EU und den USA nur konstant stabil und möglich, solange Konsumenten und Unternehmen der Stabilität des Datums vertrauen.[6]

---

1 *Reding*, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, vom 22. Januar 2017, erhältlich im Internet: <http://europa.eu/rapid/press-release_SPEECH-12-26_de.htm> (besucht am 31. Januar 2019).

2 *Bendiek/Schmied*, SWP-Aktuell, Vol. 10 (2016), 1 (2).

3 *Palmetshofer/Semsrott/Alberts*, Der Wert persönlicher Daten, Ist Datenhandel der bessere Datenschutz?, 12, vom Juni 2017, erhältlich im Internet: <https://bit.ly/2H3UhYu> (besucht am 18. März 2019).

4 *World Trade Organization (WTO)*, World Trade Report 2018, 5.

5 *Zwick/Dholakia*, Electronic Markets, Vol. 11, Issue 2 (2001), 116 (119). Ein Beispiel für den Kontrollverlust von Daten ist der Datenmissbrauch des Unternehmens Cambridge-Analytica, vgl. hierfür *Cadwalladr/Graham-Harrison,* Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, vom 17. März 2018, erhältlich im Internet: <https://bit.ly/2plU1sM> (besucht am 1. Februar 2019).

6 *Reding*, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age.

Die Snowden-Enthüllungen über die umfassende Überwachung der Bevölkerung durch die NSA erschütterten dieses Vertrauen und zogen rechtliche Konsequenzen für das transatlantische Verhältnis nach sich.[7] Am 6. Oktober 2015 erklärte der EuGH die rechtliche Grundlage des Datenaustauschs zwischen der EU und den USA, das Safe-Harbor-Abkommen und den darauf basierenden Angemessenheitsbeschluss der EU-KOMM, für ungültig.[8] Der EuGH führte als Begründung für die Entscheidung u. a. an, dass das Abhören durch die US-Geheimdienste und die entsprechende Rechtsgrundlagen den Wesensgehalt der Grundrechte auf Privatheit und Rechtsschutz von EU-Bürgern gefährden würden.[9]

Um der entstandenen Rechtsunsicherheit Einhalt zu gebieten, verhandelten EU- und US-Behörden auf Basis der EU-Datenschutzrichtlinie 94/46/EG (DSLR) das Nachfolgeabkommen Privacy Shield als derzeitigen Status quo.[10]

Seit Inkrafttreten steht das Abkommen und der ihm zugrundeliegende Angemessenheitsbeschluss der Europäischen Kommission (EU-KOMM) in der Kritik. Der im Safe-Harbour-Abkommen enthaltene Zugriff der US-Geheimdienste sei auch hier enthalten.[11] Außerdem sei die zentrale Forderung des EuGH nach unabhängigen Aufsichtsbehörden nicht verwirklicht worden und das Abkommen vom politischen Willen der US-Behörden abhängig. Insgesamt sei der Datenschutz nicht der Sache nach gleichwertig, wie es der EuGH in der Schrems-Entscheidung gefordert hatte.[12] Der Jurist und Kläger eines anhängigen Verfahrens gegen das Privacy-Shield-Abkommen, *Max Schrems*, konstatierte hierzu:

> „The deal is bad for users, which will not enjoy proper privacy protections and bad for business, which have to deal with a legally unstable solution."[13]

Wie dieser viel kritisierte und vermeintlich unsichere Status quo im transatlantischen Verhältnis aktuell rechtlich gestaltet ist und welche Probleme und evtl. Lösungen sich daraus im Kontext der DSGVO für Marktakteure in praktischen Bereichen wie Cloud-Computing, Big Data und E-Discovery ergeben, ist Thema dieser Abhandlung. Dabei wird zusätzlich erörtert werden, inwieweit rechtliche Alternativen und Lösungen für den Datentransfer auf globaler und internationaler Ebene bestehen.

[7] *Macaskill/Gabriel*, NSA Files: Decoded, What the revelations mean for you, vom 1. November 2013, erhältlich im Internet: <https://bit.ly/2dwNPcx> (besucht am 1. Februar 2019).

[8] EuGH, Rs. C362/14, *Schrems vs. Data Protection Commissioner*, Slg. 2015, ECLI:EU:C:2015:650, Rn. 107.

[9] *Ibid*., Rn. 94.

[10] Richtlinie 95/46/EG, ABl. Nr. L 281/31 vom 24. Oktober 1995, erhältlich im Internet: < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.1995.281.01.0031.01.DEU&toc=OJ:L:1995:281:TOC> (besucht am 9. Mai 2019).

[11] *European Data Protection Supervisor*, Opinion on the EU-U.S. Privacy Shield Adequacy Decision, Opinion No. 4 (2016), 3, vom 30. Mai 2016, erhältlich im Internet: <https://bit.ly/2QqSSim> (besucht am 18. März 2019).

[12] *Article 29 Data Protection Working Party (WP29)*, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 4 f., vom 13. April 2016, erhältlich im Internet: <https://bit.ly/2Fc2S7H> (besucht am 18. März 2019).

[13] *Schrems*, Privacy Shield – Press Breakfast with Jan Albrecht, vom 12. Juli 2016, erhältlich im Internet: <http://www.europe-v-facebook.org/PA_PS.pdf> (besucht am 18. März 2019).

Um dieses Thema adäquat untersuchen zu können, wird im zweiten Kapitel die Forschungsfrage in Form einer Hypothese vorgestellt, der Forschungsrahmen abgegrenzt und die angewandte Methodik erläutert. Im dritten Kapitel folgt die Darstellung und Erörterung des aktuellen Status quo vom Allgemeinen ins Spezielle. Hier wird das Vertragsverhältnis der EU und den USA zunächst in den Kontext des aktuellen internationalen Wirtschaftsrechts eingeordnet. Danach wird das Datenschutzrecht und dessen Verständnis in der USA und der EU dargelegt, um darauf basierend den aktuellen Status quo im transatlantischen Verhältnis besser diskutieren zu können. Anschließend werden im vierten Kapitel die Einflüsse und Problematiken des derzeit geltenden Rechts für Marktakteure im Bereich Cloud-Computing, Big Data und E-Discovery erörtert. Im fünften Kapitel werden derzeit mögliche Alternativen zum Privacy Shield aufgezeigt und anhand ihrer Praktikabilität eruiert. Im abschließenden Fazit wird die Forschungsfrage anhand der Ergebnisse beantwortet und ein kurzer Ausblick auf sich daraus ergebende Fragen gegeben.

B. Hypothese, Forschungsrahmen und Methodik

In diesem Kapitel wird die Forschungshypothese vorgestellt und der Forschungsrahmen definiert. Anschließend wird die Methodik erläutert, anhand derer die Hypothese beantwortet wird.

Abgeleitet von der einleitend dargestellten Kritik am derzeitigen Privacy-Shield-Abkommen und angeleitet, die oben gesteckten Themen zielgerichtet zu untersuchen, wird sich in dieser Arbeit an folgender Hypothese abgearbeitet:

Die aktuellen Regulierungen des Datenschutzes im transatlantischen Verhältnis hinken den rechtlichen Anforderungen hinterher und fördern damit Rechtsunsicherheit und Risiken für Unternehmen und deren Kunden.

Um diese These im Rahmen dieser Untersuchung angemessen be- oder widerlegen zu können, beschränkt sich diese auf die aktuellen Regulierungen und Quellen im transatlantischen Datenschutzverhältnis bis einschließlich Februar 2019. Dazu gehören das Allgemeine Abkommen über den Handel mit Dienstleistungen (GATS), das Privacy-Shield-Abkommen, die DSGVO, die DSLR, US-Gesetze sowie relevante Gerichtsentscheidungen und andere Primärquellen.[14]

Die betrachteten praktischen Komplexe sind Cloud-Computing, Big Data und E-Discovery. Die benannten Begriffe werden dazu in den sie betreffenden Kapiteln definiert. Andere interessante Bereiche wie z. B. das Kartellrecht sind nicht weniger relevant, werden aber des Umfangs wegen von der Untersuchung ausgeschlossen.

Um die Hypothese zu bearbeiten, werden die oben genannten Primärquellen mithilfe von einschlägiger Primär- und Sekundärliteratur wie Urteilen, Kommentierungen und Studien eingeordnet und diskutiert.

[14] Da es sich nur um einen Querschnitt zum definierten Zeitpunkt handelt, begrenzt sich die Validität der Schlussfolgerungen auf den abgesteckten Rahmen der Untersuchung.

C. Status quo: GATS, die EU und Privacy Shield

Um den aktuellen Status quo und seine Problematik zu erfassen, wird in diesem Kapitel das Privacy-Shield-Abkommen zwischen der EU und den USA in den Kontext der relevanten supranationalen, internationalen und nationalen Rechtsregime gestellt.

I. Art. XIV GATS: Völkerrechtliche Grundlage des Datenschutzes

Den völkerrechtlichen Rahmen für Regelungen des Datenaustauschs zwischen den USA, der EU und ihren Mitgliedern kodifiziert das 1995 in Kraft getretene GATS.[15]

Gemäß Art. I Abs. 2 lit. a) GATS unterliegt der grenzüberschreitende Austausch und Handel von Daten zwischen den beiden Mitgliedern mindestens einer der vier Kategorien von grenzüberschreitenden Dienstleistungen, die das GATS in Art. I Abs. 2 reguliert.[16] War die technische Entwicklung 1995 weit von dem entfernt, was heute als normal gilt, lassen die offenen Definitionen des Artikel I GATS dies zu.[17]

Nichtsdestotrotz kann kritisch angemerkt werden, dass das WTO-Recht im Allgemeinen und das GATS im Speziellen angesichts der exponentiellen Technikentwicklung und der Bedeutung des Datenhandels im Dienstleistungsbereich als reformbedürftig gesehen werden können.[18]

Ratio des GATS ist es, den liberalen Handel als Mittel der Wohlstandsförderung und mittelbaren Friedensstifter multilateral zu fördern. Um sich diesem Ziel zu nähern, sollen zwischen den WTO-Mitgliedern tarifäre und nicht-tarifäre Handelshemmnisse im Dienstleistungsbereich abgebaut werden.[19] Hierzu gehören Zölle, aber auch das grundsätzliche Verbot offener und versteckter Diskriminierungen von WTO-Mitgliedern gegenüber anderen WTO-Mitgliedern. Dies sind Regulierungen, die der Sache nach gleiche Dienstleistungen – in diesem Fall Datentransfers – ohne sachlichen Grund besser- oder schlechterstellen und damit dem Ziel des liberalen Handels widersprechen.[20] Dieser Grundsatz wird u. a. durch das Meistbegünstigungsprinzip (MFN) in Art. II Abs. 1 GATS kodifiziert.

Verstöße einer Vertragspartei gegen diesen Grundsatz sind legitim, sofern die evtl. diskriminierende Maßnahme des Mitgliedstaats durch einen Rechtfertigungsgrund gedeckt ist und sie für das Erreichen des Regulierungsziels erforderlich ist.[21]

15 *F. Weiss*, in: Tietje (Hrsg), Internationales Wirtschaftsrecht, 237 (265 f.). Die unmittelbare Wirkung des GATS für Mitgliedsstaaten der EU hat der EuGH jedoch in seiner ständigen Rechtsprechung verneint. Vgl. dafür *ibid.*, 268.

16 *Chaner*, *in: WTO* (Hrsg), World Trade Report 2018, 194 (194).

17 *Bendiek/Schmied*, SWP-Aktuell, Vol. 10 (2016), 1 (3).

18 *WTO*, World Trade Report 2018, 12.

19 *F. Weiss*, in: Tietje (Hrsg), Internationales Wirtschaftsrecht, 237 (240 f.). Sowie Art. XIX Abs. 1 des Allgemeinen Übereinkommens über den Handel mit Dienstleistungen (GATS).

20 *Ibid.*, 237 (245).

21 *Wiegemann*, Die Liberalisierung des Dienstleistungshandels, 189 f.

Als Rechtfertigungsgrund der Datenschutzregulierung zwischen USA und EU könnte Art. XIV lit. c) ii) GATS maßgeblich sein:

> „Unter der Voraussetzung, daß [sic!] Maßnahmen nicht in einer Weise angewendet werden, die ein Mittel zur willkürlichen oder unberechtigter Diskriminierung unter Ländern, in denen gleiche Behandlung herrschen, oder eine verdeckte Beschränkung für den Handel mit Dienstleistungen darstellen würde, darf dieses Übereinkommen nicht dahingehend ausgelegt werden, daß [sic!] es die Annahme oder Durchsetzung von Maßnahmen eines Mitglieds verhindert,
> c) die erforderlich sind, um die Einhaltung von Gesetzen oder sonstigen Vorschriften zu gewährleisten, die nicht im Widerspruch zu diesem Übereinkommen stehen, einschließlich solcher
> ii) zum Schutz der Persönlichkeit bei der Verarbeitung und Weitergabe personenbezogener Daten und zum Schutz der Vertraulichkeit persönlicher Aufzeichnungen und Konten."[22]

Es fehlt bis heute ein Verfahren vor dem Dispute Settlement Body (DSB) der WTO, der sich im Falle eines Verfahrens mit der Rechtmäßigkeit einer Datenschutzregulierung beschäftigen würde. Art. XIV GATS ist den allgemeinen Ausnahmen des Art. XX GATT nachempfunden.[23] Aus diesem Grund lassen sich aus einschlägigen Entscheidungen zum Art. XX GATT die Schranken ableiten, die der Privacy Shield, die DSGVO und andere Datenschutzregulierungen nehmen müssten, käme es zu einem Verfahren.

Demnach müsste die Maßnahme der in der Entscheidung *US-Gambling Services* entwickelten, zweistufigen Überprüfung standhalten.[24] In dieser wird grundsätzlich geprüft, ob die Maßnahme erforderlich ist.

Hierzu würde im ersten Schritt überprüft werden, ob ein kausaler Zusammenhang zwischen der Datenschutzregulierung und ihrem Ziel besteht.[25] Um dem zuzustimmen, könnte argumentiert werden, dass durch den Privacy Shield die Privatsphäre von Betroffenen als Schutzgut geschützt wird. Dürfen Daten nur zweckgebunden erhoben werden, wie es im fünften Prinzip des Privacy Shield festgelegt ist, hätte dies in der Summe weniger erhobene Daten zur Folge.[26] Weniger Daten bedeuten weniger Risiko einer Kompromittierung der Privatsphäre von Betroffenen.[27]

Im zweiten Schritt würde geprüft, ob die Datenschutzregulierungen die am wenigsten handelsbeschränkenden sind. Das heißt, ob es eine alternative Regulierung gäbe, die bei selbigem Schutz der Privatsphäre das GATS weniger verletzt würde.[28] Seit der *Korea-Beef*-Entscheidung wird hierbei abgewogen, ob die Datenschutzregulierung einen eher unverzichtbaren Beitrag für den Schutz der Privatsphäre leistet. Je höher hierbei das Allgemeininteresse am Schutz der Privatsphäre wöge, desto größer der Beitrag der Regulierung zur Durchsetzung des Letzteren. Je geringer das Ausmaß

22 Art. XIV lit. c) ii) GATS. Hervorhebung durch den Autor.
23 *Wiegemann*, Die Liberalisierung des Dienstleistungshandels, 181.
24 *Lester/Mercurio/Davies*, World Trade Law, 699.
25 *Wiegemann*, Die Liberalisierung des Dienstleistungshandels, 190 f.
26 *U.S. Department of Commerce*, EU-US Privacy Shield Principles issued by the U.S. Department of Commerce, erhältlich im Internet: <https://bit.ly/2JkaKsR> (besucht am 18. März 2019), 6.
27 Unter anderem wurde auch aus diesem Grund das sog. Datenminimierungsprinzip in der DSGVO kodifiziert, vgl. dazu Art. 5 Abs. 1 lit. c) der Verordnung Nr. 2016/679, ABl. EG Nr. L 119/35 vom 27. April 2016, erhältlich im Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679> (besucht am 9. Mai 2019).
28 *Wiegemann*, Die Liberalisierung des Dienstleistungshandels, 192 f.

der Handelsbeschränkung wäre, desto erforderlicher der Privacy Shield in diesem Fall.[29]

Hierzu könnte angeführt werden, dass das Gegenteil einer Regulierung, ein nicht regulierter Austausch von Daten zwischen den USA und der EU, in der Vergangenheit schon zu Vorfällen wie dem Cambridge-Analytica-Skandal geführt hat. Dieser hatte die Privatsphäre von 50 Millionen Betroffen kompromittiert und in diesem Sinne auch das Allgemeininteresse des Schutzes der Privatsphäre berührt.[30] Weiter könnte zum Allgemeininteresse angeführt werden, dass in beiden Wirtschaftszonen die (digitale) Privatsphäre und die dafür notwendige Sicherheit von Daten als Bedingung für das Funktionieren einer Marktwirtschaft mit geistigem Eigentum als wesentliche Währung notwendig ist.[31] Als Gegenargument könnten z. B. das höhere Potenzial für Innovationen durch ungehinderten Datenaustausch angeführt werden, das durch diese Regulierung behindert werden könnte.

Im Ergebnis gab es jedoch noch kein entsprechendes Verfahren. Insofern ist das oben beschrieben Gedankenspiel rein spekulativ und dessen Argumente nur sehr verkürzt und nicht erschöpfend dargestellt. Festgehalten werden kann aber, dass die EU und die USA als Vertragsparteien sich an das GATS als völkerrechtlichen Rahmen halten müssen.[32] Dabei lässt das GATS durch Art. XIV wohl den Raum für supranationale, internationale und nationale Datenschutzregulierungen, wie auch der ehem. Datenschutzbeauftragte des Landes Berlin, *Alexander Dix*, argumentiert.[33]

Wie dieser Raum in den USA gestaltet ist und welche Aspekte im Verhältnis zur EU für Marktakteure letztendlich problematisch sein könnten, wird im nächsten Kapitel diskutiert.

II. „Flickenteppich“: Die USA

In seinem modernen Verständnis hat das Recht auf Privatsphäre seinen Ursprung in den USA. Schon 1890 beschrieben die Juristen *Samuel Dennis Warren* und *Louis Brandeis* in ihrem Aufsatz „The Right to Privacy“ heute im Datenschutz maßgebliche Grundsätze wie Zweckbindung und Erforderlichkeit.[34]

Die derzeitige Regulierung des US-Datenschutzes wird jedoch nicht selten als sog. Flickenteppich beschrieben.[35] Hiermit ist gemeint, dass es im Gegensatz zur EU keine bundesweite, einheitliche Regulierung äquivalent zur DSLR oder der DSGVO gibt. Stattdessen setzt der Bundesgesetzgeber in den USA auf spezielle, dem jeweiligen Sek-

[29] *Ibid.*, 195 f.
[30] *Cadwalladr/Graham-Harrison*, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, vom 17. März 2018, erhältlich im Internet: <https://bit.ly/2plU1sM> (besucht am 18. März 2019).
[31] *Bendiek/Schmied*, SWP-Aktuell, Vol. 10 (2016), 1 (8).
[32] Art. 216 Abs. 2 AEUV.
[33] *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (8 f.).
[34] *Schmitz*, in Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 2, Rn. 8.
[35] *M. Weiss/Archick*, U.S.-EU Privacy: From Safe Harbor to Privacy Shield, Congressional Research Report, No. R44257, 3 f., vom 19. Mai 2016, erhältlich im Internet: <https://bit.ly/2PVPqt9> (besucht am 18. März 2019).

tor angepasste Regulierungen. Hinzu kommen Regulierungen der einzelnen Bundestaaten.[36]

Das Recht auf Privatsphäre als Quell und Voraussetzung einer freiheitlichen Demokratie ist fest in der US-Verfassung verankert. Auf Bundesebene sind für den US-Datenschutz vor allem der vierte und der erste Verfassungszusatz einschlägig. Der vierte Verfassungszusatz garantiert US-Staatsbürgern und deren Privatsphäre Schutz vor staatlichen Übergriffen in Form von willkürlichen Durchsuchungen oder Festnahmen.[37] Der erste Verfassungszusatz schützt unter anderem das Recht auf Meinungsfreiheit.[38] Der Eingriff in diesen Schutzbereich steht unter Richtervorbehalt.[39] Diesen Schutz genießen nur US-Staatsbürger, er entfaltet keine Drittwirkung.[40] Im Hinblick auf den Datenschutz von EU-Staatsbürgern und/oder Geschäftsgeheimnisse von EU-Unternehmen in den USA könnte dies problematisch sein.

Der technischen Entwicklung Rechnung tragend, entwickelte der US-Gesetzgeber im US Privacy Act von 1974 und im Electronic Communications Act von 1986 gesetzliche Schranken und ggf. Rechtsmittel für US-Bürger beim Umgang mit elektronisch übertragenen, personenbezogenen Daten im öffentlichen Bereich. Diese Rechtsmittel standen ebenfalls bis zuletzt nur US-Bürgern zu.[41]

Nachdem der EuGH in der Schrems-Entscheidung fehlende Rechtsmittel für EU-Bürger bemängelte, reagierte der US-Gesetzgeber mit dem Judicial Redress Act 2016. In diesem wurden die im Privacy Act vorhanden Rechtsmittel gegen Überwachung auf EU-Bürger und Bürger anderer zertifizierter Staaten ausgeweitet.[42] Hierbei muss angemerkt werden, dass die angesprochenen Rechtmittel im Privacy Act, also auch im Judicial Redress Act, schwach ausgeprägt sind.[43] So können Verfahren durch den Generalanwalt nur mit Übereinstimmung des Vorsitzenden der vom Verfahren betroffenen Behörde eingeleitet werden.[44] Inwieweit hier effektiver Rechtschutz möglich ist, kann durchaus hinterfragt werden.[45]

Im privaten Sektor sind bereichsspezifische Regulierungen vorherrschend. Sie prägen das angesprochene Bild des Flickenteppichs gegenüber dem allgemeinen und allumfassenden Ansatz der EU. Dessen Lücken und das Fehlen einer flächendeckenden

36 *Ibid*.
37 *Ad-Hoc EU-US Working Group on Data Protection,* Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, 3, vom 27. November 2013, erhältlich im Internet: <https://bit.ly/2W6MAnd> (besucht am 18. März 2019).
38 Verfassung der USA, 1. Zusatzartikel.
39 *Ad-Hoc EU-US Working Group on Data Protection*, Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, 3 f.
40 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (134).
41 *M. Weiss/Archick*, U.S.-EU Privacy: From Safe Harbor to Privacy Shield, Congressional Research Report, No. R44257, 3 ff.
42 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (129).
43 *Krempl*, Datenschutz: EU-Bürger erhalten theoretische Klagemöglichkeit in den USA, vom 25. Februar 2019, erhältlich im Internet: <https://www.heise.de/newsticker/meldung/Datenschutz-EU-Buerger-erhalten-theoretisch-Klagemoeglichkeit-in-den-USA-3117699.html> (besucht am 12. März 2019).
44 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (130).
45 *Ibid.*, 129.

Regulierung wird von Datenschützern in den USA oft kritisiert, von Befürwortern allerdings oft als Wettbewerbs- und Innovationsvorteil beschrieben.[46]

Grundsätzlich kann festgehalten werden, dass im Datenschutz die unterschiedlichen Philosophien von Privatsphäre und damit unterschiedliche Regulierungen der Internetökonomie zur Geltung kommen. Der US-Ansatz setzt gegenüber dem EU-Ansatz seit Anfang der 2000er Jahre verstärkt auf Selbstregulierung und Selbstzertifizierung der Internetökonomie anstelle von Regulierung, oder pointiert formuliert: Auf die Freiheit des Datenhandels, statt dessen Kontrolle.[47]

Weitergedacht werden Daten auf dem freien Markt – vereinfacht und abstrakt dargestellt – als handelbares Gut betrachtet, und nicht als Eigentum der natürlichen Personen hinter den Daten. Folglich werden Daten nicht dem Eigentümer als Quelle, sondern dem Markt unterstellt. Als Konsequenz entscheidet auch nicht der Eigentümer als einziger Souverän und Rechteträger über den Austausch der Besitzrechte an den Daten, sondern der Markt. In kürze und überspitzt formuliert wird dadurch das Datum als Teil der Privatsphäre zum handelbaren Gut und damit von seinem eigentlichen Standort entkoppelt: Dem Menschenrecht.[48]

In der Praxis lässt sich dieser bereichsspezifische, marktorientierte Ansatz an der Legaldefinition der Datenverarbeitung festmachen. Diese ist im Gegensatz zur EU-Regulierung nicht weit gefasst, betrifft also nicht alle Schritte in der Datenverarbeitungskette, sondern setzt je nach Sektor an verschiedener Stellen des Verarbeitungsprozesses an.[49] Das heißt zum Beispiel, dass eine Datenspeicherung in den USA je nach Bundesstaat nicht immer eine Datenverarbeitung im i. S. d. Gesetzes darstellt und damit nicht in den Anwendungsbereich der Datenschutzgesetze fällt.[50] Oder, dass IP-Adressen und pseudonymisierte Daten im Gegensatz zur EU nicht in den Anwendungsbereich der Datenschutzgesetze fallen.[51]

Einerseits entstand hierdurch ein unternehmens- und innovationsfreundliches Klima und damit das Epizentrum der vierten industriellen Revolution, das Silicon Valley. Andererseits trug dieser weitreichende Spielraum auch zur Marktdominanz der großen vier Unternehmen Google, Apple, Facebook und Amazon (sog. GAFA) bei.[52]

46 *Zwick/Dholakia*, Electronic Markets, Vol. 11, Issue 2 (2001), 116 (119 f.).
47 *Ibid.*, 119 f.
48 *Ibid.*, 117 ff.
49 *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 11 ff.; Art. 2 Abs. 1 DSGVO.
50 *Ad-Hoc EU-US Working Group on Data Protection*, Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, 9, vom 27. November 2013, erhältlich im Internet: <https://bit.ly/2W6MAnd> (besucht am 18. März 2019).
51 *Voss*, Journal of Internet Law, Vol. 19, No. 11 (2016), 1; 9 (14).
52 Für Googles Marktdominanz vgl. *Statista GmbH*, Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung im Februar 2019, vom Februar 2019, erhältlich im Internet: <https://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/> (besucht am 18. März 2019);
Für Facebooks Marktdominanz vgl. *Statista GmbH*, Marktanteile von Social Media Seiten nach Seitenabrufen weltweit von Dezember 2018 bis Februar 2019, erhältlich im Internet: <https://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit/> (besucht am 18. März 2019);
Für Amazons Marktdominanz vgl. *Statista GmbH*, Anteil des Umsatzes von Amazon am gesamten Online-Handelsumsatz in Deutschland in den Jahren 2008 bis 2016, erhältlich im Internet: <https://de.statista.com/statistik/daten/studie/669851/umfrage/marktanteil-von-amazon-im-online-handel-in-deutschland/> (besucht am 18. März 2019).

Problematisch hieran könnte die Konzentration von Daten und somit die Kontrolle dieser innerhalb weniger Unternehmen gegenüber vielen Kunden sein. Die Kunden nehmen in einem eher auf unternehmerische Freiheit orientierten Datenmarkt eine passive Rolle ein. Sie haben keine Kontrolle, *ergo* auch keine Souveränität über die Verwendung des Datums selbst. Abstrakt formuliert befinden sich die Konsumenten in einer asymmetrischen Machtsituation gegenüber dem handelnden Unternehmen. Als Folge können sie nicht mehr entscheiden, wer, was, wann mit ihren Daten macht, weil ihnen das US-Datenschutzrecht keine aktive Teilhabe garantiert oder es je nach bereichsspezifischer Regulierung nicht greift.[53]

Begünstigt durch diese Passivität ist in den USA die sog. Data-Broker-Industrie entstanden. Diese werden als Dritthändler von Daten beschrieben, deren Geschäftsgrundlage das teilweise für den Konsumenten undurchschaubare Handeln mit Daten und somit das Ausnutzen der oben beschriebenen Datenschutzasymmetrie ist.[54]

Die Reichweite dieses Datenhandels ist dabei nicht auf die USA beschränkt, sondern global und damit auch für das Verhältnis zur EU relevant. Dem US-Kongress nach waren im Jahr 2013 47 von 100 Unternehmen der Fortune 100, 12 der 15 führenden Kreditunternehmen und acht der zehn führenden Telekommunikationsunternehmen Kunden des markführenden Datenhändlers Axciom.[55]

Umrahmt werden die auf US-Bürger beschränkten Abwehrrechte und das bereichsspezifische, eher marktorientierte Datenschutzrecht von Zugriffsrechten der US-Sicherheitsbehörden, die der breiten Öffentlichkeit durch die Enthüllungen von *Edward Snowden* bekannt wurden.

Einschlägige US-Rechtsgrundlagen hierzu sind der Patriot Act, die Executive Order 12333 (EO 12333), die Presidential Policy Directive 28 (PPD-28), die Section 702 des Foreign Intelligence Surveillance Acts (FISA) und der 2018 in Kraft getretene Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[56]

Bietet der Patriot Act neben Drittstaatsbürgern auch die Rechtsgrundlage für den Zugriff auf Daten von US-Bürgern, regulieren die EO 12333 und die PPD-28 den Zugriff auf Daten von Drittstaatsbürgern zum Zweck der geheimdienstlichen Informationsgewinnung.[57] Die Kompetenz für den Zugriff auf Daten von Drittstaatsbürgern wird mit der verfassungsgegebenen, inhärenten Autorität des US-Präsidenten als Oberbefehlshabers gerechtfertigt.[58]

Die sog. geheimdienstliche Informationsgewinnung ist hierbei als Rechtfertigung der Überwachung in der PPD-28 sehr weit gefasst. Demnach ist die sog. Bulk-Collection von Daten, also eine allumfassende Erfassung der Daten von Drittstaatsbürgern, u. a. gerechtfertigt, wenn es um Informationen über Spionage gegen die

53 *Schütz/Karaboga*, Regulierungspraxis im Datenschutz, 7 f.
54 *Crain*, New Media & Society, Vol. 20, Issue 1 (2018), 88 (93).
55 *U.S. Senate Committee on Commerce, Science & Transportation,* A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, 29, vom 18. Dezember 2013, erhältlich im Internet: <https://bit.ly/2W7VmkR> (besucht am 18. März 2019).
56 *EU-Parliament, Committee on Civil Liberties, Justice Home Affairs*, Background note on US legal Instruments for access and electronic surveillance of EU citizens, 1 f., erhältlich im Internet: <https://bit.ly/2UHY8go> (besucht am 18. März 2019).
57 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (120).
58 *Ibid.; Ad-Hoc EU-US Working Group on Data Protection*, Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, 3.

USA und ihre Interessen, internationalen Terrorismus, Massenvernichtungswaffen, Bedrohungen der USA und/oder Alliierter und transnationale Bedrohungen geht.[59] Inwiefern diese Zweckorientierung eine Beschränkung enthält, ist also durchaus diskutabel.

Die oben beschriebenen verfassungsgemäßen Grenzen des vierten und ersten Zusatzartikels der US-Verfassung gelten im Falle der EO 12333 und der PPD-28 nur für US-Bürger und solche Drittstaatsbürger, die in den USA sesshaft sind.[60]

Gleiches gilt für Section 702 des FISA und den 2018 in Kraft getretenen CLOUD Act. Beide sind Rechtsgrundlagen für den Zugriff auf Daten von Drittstaatsbürgern über Internetdienstanbieter (ISPs), die sich aller Voraussicht nach außerhalb der USA aufhalten.[61] ISPs wie Apple oder Dropbox müssen bei gegebener Rechtsgrundlage – der nationalen Sicherheit – den Zugriff ermöglichen.[62] Die auf FISA basierende Überwachung wurde als PRISM öffentlich bekannt.[63]

Die Überprüfung und Legitimität der auf Section 702 FISA basierend Zugriffe wird hierbei jährlich und *ex parte* vom United States Foreign Intelligence Surveillance Court (FISC) vorgenommen.[64] Das FISC prüft hierbei, ob die zu sammelnden Daten relevant für eine Untersuchung sind, sie keinen US-Bürger betreffen und gegen internationalen Terrorismus bzw. gefährliche Aktivitäten schützen. Für die Relevanz der Daten kann auch deren potenzieller Wert in der Zukunft für die Abwehr der genannten Gefahren herangezogen werden.[65] Beschlüsse des FISC sind geheim, sofern sie die nationale Sicherheit betreffen. ISPs dürfen in einem solchen Fall Betroffene nicht über die Herausgabe informieren. Rechtsmittel existierten entsprechend lt. EU-Arbeitsgruppe 2013 für Drittstaatsbürger keine.[66] Dies bestätigte der US-Supreme Court in der Entscheidung *Clapper vs. Amnesty International*.[67] Bis heute werden die fehlenden Rechtsmittel im Verhältnis zur EU kritisiert.[68] 2015 wurde als Reaktion durch eine Reform des FISA der Datenminimierungsgrundsatz in die FISC-Entscheidung einbezogen.[69]

Zusammengefasst hat das Datenschutzrecht der USA mit seinem verfassungsgegebenen Schutz der Privatsphäre den für die USA typischen Charakter eines negativen

59 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (121).
60 *Ibid.; Ad-Hoc EU-US Working Group on Data Protection*, Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, 17.
61 *Mewes*, CLOUD Act – US-Gesetz für internationalen Datenzugriff und -schutz verarbschiedet, vom 24. März 2018, erhältlich im Internet: <https://www.heise.de/newsticker/meldung/CLOUD-Act-US-Gesetz-fuer-internationalen-Datenzugriff-und-schutz-verabschiedet-4003330.html?wt_mc=rss.ho.beitrag.atom> (besucht am 18. März 2019).
62 *Ad-Hoc EU-US Working Group on Data Protection*, Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, 3.
63 *Ibid.*
64 *Ibid.*, 3,12.
65 *Ibid.*, 12.
66 *Ibid.*, 16 f.
67 *Ibid.*
68 Siehe dafür Kapitel C IV.
69 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (120).

Abwehrrechts.[70] Die zur Verfügung stehenden Rechtsmittel beschränken sich auf US-Bürger, was im Verhältnis zur EU problematisch sein könnte.

Zudem ermöglichte der US-Gesetzgeber mit einer bereichsspezifischen, marktorientierten Regulierung im privaten Bereich die Entstehung der modernen Internetökonomie. Gleichzeitig ist er jedoch mitverantwortlich für die Informations- und Kontrollasymmetrie von Konsumenten gegenüber Unternehmen im Datenmarkt. Besonders die unterschiedlich definierten, eher eng gefassten Anwendungsbereiche des Datenschutzrechts der USA könnten im Verhältnis zum allumfassenden Ansatz EU problematisch sein. Entsprechend erscheint das postulierte Bild des Flickenteppichs treffend.

Hinzu kommen die beschriebenen Zugriffsrechte auf Daten von EU-Bürgern außerhalb des US-Staatsgebiets ohne zugehörige – oder im Fall des Judicial Redress Acts nur sehr beschränkte Rechtsmittel.

Welchen Charakter die EU-Regulierungen im Verhältnis zum beschriebenen US-Datenschutz aufweisen, wird im folgenden Kapitel analysiert.

III. Datenschutz als Grundrecht in der EU: DSLR und DSGVO

Als erste Datenschutzregulierung auf EU-Ebene trat 1995 die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSRL) in Kraft.[71] Zuvor hatten bereits sieben der 12 damaligen EU-Mitglieder Datenschutzgesetze kodifiziert. Auch internationale Organisationen wie der Europarat mit seiner Datenschutzkonvention von 1981, die OECD und die Vereinten Nationen hatten bereits Leitbilder für den Datenschutz formuliert.[72] Vor allem die Datenschutzkonvention des Europarats war Orientierung für den EU-Gesetzgeber. Sie enthielt u. a. die heute als Standard empfundenen Pflichten zur Richtigkeit und Aktualität von Daten sowie Legaldefinitionen von grundlegenden Begriffen wie personenbezogenen Daten, die ebenfalls in der DSGVO zu finden sind.[73]

Ziel der DSRL war es, im Zuge der Binnenmarktharmonisierung die Regulierung des Datenschutzes zu vereinheitlichen. Die Verhinderung des Zugriffs unbefugter Dritter auf personenbezogene Daten sollte EU-weit in einem allgemeinen Regelwerk kodifiziert werden. Durch die Rechtsform der Richtlinie wurde den EU-Mitgliedern hierbei jedoch noch Gestaltungsfreiheit auf dem Weg zur Zielerreichung gegeben.[74] Ihre Grenzen hatte und hat die mitgliedsstaatliche Gestaltungsfreiheit in der Pflicht zur richtlinienkonformen Auslegung bzw. Umgestaltung des nationalen Rechts zur Zielerreichung.[75]

Entscheidend für die europäische Vorstellung eines Grundrechts auf Datenschutz und somit auch für die Urteile des EuGHs war die Entwicklung des EU-Primärrechts.

[70] *Schütz/Karaboga*, Regulierungspraxis im Datenschutz, 7 f.
[71] Richtlinie 95/46/EG, ABl. EG Nr. L 281/31 vom 24. Oktober 1995.
[72] *Schulte*, Vom quantitativen zum qualitativen Datenschutz, 113 ff.
[73] *Ibid.*, 124.
[74] Art. 288 Abs. 3 AEUV; *Herdegen*, Europarecht, § 8, Rn. 46.
[75] *Ibid.*, Rn. 50.

Für den europäischen Datenschutz ist hierbei die Entstehung Charta der Grundrechte der Europäischen Union (GRCh) im Jahr 2000 mit Art. 8 Abs. 1 GRCh hervorzuheben.

„Art. 8 Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschrift wird von einer unabhängigen Stelle überwacht."[76]

Die GRCh bindet seit ihrer primärrechtlichen Inkorporierung durch den Vertrag von Lissabon die Union und ihre Organe.[77] Die EU-Mitgliedsstaaten sind nach dem Grundsatz der loyalen Mitwirkung entsprechend an die Grundrechtecharta, die Verträge und das davon abgeleitete Sekundärrecht gebunden.[78] Dem EuGH obliegt hierbei im Rahmen des Vorabentscheidungsverfahrens die ausschließliche Kompetenz, über die Verträge der Union und die Gültigkeit des Sekundärrechts wie der DSGVO zu entscheiden.[79] Gerichte der EU-Mitgliedsstaaten haben entsprechend bei Fragen zur Auslegung der Verträge oder des Sekundärrechts gem. Art 267 eine Vorlageverpflichtung gegenüber dem EuGH.[80] Im Lichte einer EuGH-Entscheidung obliegt den nationalen Gerichten dann die Aufgabe, nationales Recht unionsrechtskonform auszulegen.[81] Als Konsequenz wurde das europäische Datenschutzrecht maßgeblich durch den EuGH und seine Entscheidungen fortgeschrieben und ausgeweitet.[82]

Trotz Ergänzung u. a. durch die Richtlinie für elektronische Kommunikation und Fortentwicklung des Datenschutzrechts durch den EuGH, wurde die DSLR durch ihr Alter reformbedürftig.[83] Auf Basis des Art. 16 AEUV trat die DSGVO nach einer zweijährigen Übergangsfrist am 25. Mai 2018 an ihre Stelle. Die DSGVO bedarf gem. Art. 288 Abs. 2 AEUV keinerlei nationaler Umsetzung, gilt unmittelbar, ist in allen Teilen für die Mitgliedstaaten der EU verbindlich und hat Anwendungsvorrang vor nationalem Recht.[84] Entsprechend können sich EU-Bürger als natürliche Personen durch die unmittelbare Anwendbarkeit auf sie berufen.[85]

[76] Art. 8 der Charta der Grundrechte der Europäischen Union, ABl. EG Nr. C 364/10 vom 18. Dezember 2000.

[77] Art. 6 Abs. 1 EUV; *Herdegen*, Europarecht, § 8, Rn. 24.

[78] Art. 4 Abs. 3 EUV; *Herdegen*, Europarecht, § 6, Rn. 14.

[79] *Ibid*., § 9, Rn. 25 ff.

[80] *Ibid*., § 9, Rn. 26.

[81] *Ibid.,* § 9, Rn. 27.

[82] *Ibid.,* § 8, Rn. 27 f.

[83] Richtlinie 2002/58/EG, ABl. EG Nr. L 201/37 vom 31. Juli 2002, erhältlich im Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32002L0058&from=DE> (besucht am 9. Mai 2019).

[84] Grundsatzentscheidung für den sog. Anwendungsvorrang des Unionsrechts war die Entscheidung *Costa/E.N.E.L.* des EuGH, Rs. 6/64, *Costa/E.N.E.L.,* Slg. 1964, EU:C:1964:66, vgl. dazu *Herdegen*, Europarecht, § 10, Rn. 1.

[85] *Moos/Schefzig*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 1, Rn. 5; Europarechtlich grundlegend für das Prinzip der unmittelbaren Anwendbarkeit war die Entscheidung *van Gend & Loos* des EuGHs, vgl. dazu *Herdegen*, Europarecht, § 8, Rn. 13; 44; sowie EuGH, Rs. 26/62, *van Gend & Loos*, Slg. 1963, EU:C:1963:1.

Gem. Art. 95 DSGVO gilt normhierarchisch die Richtlinie für elektronische Kommunikation als *lex specialis* zur DSGVO fort.[86] Nationale Regelungen, die der Umsetzung des Ziels der Richtlinie dienen, haben Vorrang zur DSGVO. Alle anderen, nicht von einer Öffnungsklausel betroffenen nationalen Gesetze, werden durch den Anwendungsvorrang verdrängt.[87] Durch die sog. Öffnungsklauseln der DSGVO besteht dennoch Spielraum für Konkretisierungen und spezielle Regelungen der Mitgliedsstaaten.[88] In Relation zum „Flickenteppich" USA könnte also durchaus behauptet werden, dass der Datenschutz in Europa ebenfalls ein Regelungsgeflecht darstellt, das auf Anwenderseite für Rechtsunsicherheit sorgen kann.[89]

Der Name „Grundverordnung" steht hierbei für Ziel und Ansatz des Gesetzgebers. Im Gegensatz zum bereichsspezifischen, eng gefassten Anwendungsbereich der Datenschutzgesetzgebung in den USA erfasst der Schutzbereich der DSGVO „jede" Verarbeitung personenbezogener Daten.[90] Der Anwendungsbereich umfasst den gesamten Verarbeitungsprozess eines personenbezogenen Datums entlang seiner Existenz. Dazu gehören u. a. das Erheben, Erfassen, Ordnen, Speichern, die Organisation, die Anpassung, das Abrufen, die Übermittlung und das Vernichten eines personenbezogenen Datums.[91] Der offene, technikneutrale Wortlaut entspricht also dem Ziel, den Schutzbereich der DSGVO weitreichend, zukunftssicher und vor allem allgemein zu definieren.[92]

Allerdings gibt es auch Kritiker dieses Ansatzes. Die Allgemeinheit der Formulierung trage den technischen Anforderungen spezieller Anwendungen wie z. B. Cloud-Computing zu wenig Rechnung. Innovationen seien so weniger möglich.[93] Hiergegen könnte man anführen, dass eine Grundverordnung ihrem Wesen nach gerade keine Ansprüche darauf erhebt, spezielle Regelungen zu treffen. Die in der DSGVO enthaltenen Öffnungsklausen eröffnen dabei trotzdem jenen Spielraum für spezielle, nationalstaatliche Regelungen.[94] Ein Beispiel hierfür ist Art. 88 Abs. 1 DSGVO. Art. 88 Abs. 1 DSGVO eröffnet Freiheiten für nationalstaatliche Regelungen hinsichtlich der Datenverarbeitung im Beschäftigungskontext. Aus diesem Grund wird die DSGVO auch als Verordnung mit Richtliniencharakter eingeordnet, die eher einen kleinsten gemeinsamen Nenner als eine Vollharmonisierung darstellt.[95]

86 *Moos/Schefzig*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 1, Rn. 10 f.

87 *Ibid.*

88 Die sog. Öffnungsklauseln sind dabei in drei Kategorien unterteilt, in denen der nationale Gesetzgeber die DSGVO konkretisieren, ergänzen oder modifizieren kann. Die DSGVO-Konformität ist hierbei seitens der EU-Mitgliedsstaaten immer zu beachten. Vgl. hierzu *Bremann,* Öffnungsklauseln der DSGVO: Welche Gesetze gehen vor, vom 16. Februar 2018, erhältlich im Internet: <https://bit.ly/2TU3vMu> (besucht am 15 März 2019).

89 *Moos/Schefzig*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 1, Rn. 14.

90 Art. 4 Nr. 2 DSGVO.

91 Art. 2 Abs. 1 DSGVO i. V. m. Art. 4 Nr. 2 DSGVO.

92 *Meyerdierks*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 140.

93 *Ibid.*

94 *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 289.

95 *Culik*, in: Hoeren/Kolany-Raiser (Hrsg), Big Data, 29 (29; 31); *Gilbert*, EU General Data Protection Regulation: What Impact for Businesses Established Outside the EU,

Im Gegensatz zur USA gilt ein grundsätzliches Verbot mit Erlaubnisvorbehalt für die Verarbeitung von personenbezogenen Daten.[96] Personenbezogene Daten werden dabei als „[...] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen [...]" definiert.[97]

> „Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."[98]

Einerseits wird hiermit die Berufung auf die DSGVO auf natürliche Personen oder die sie vertretenen NGOs reduziert.[99] Andererseits wurde durch den Wortlaut „[...] direkte oder indirekte, insbesondere mittels Zuordnung" ein relativer Datenschutz eingeführt. [100] Beispielsweise ist es möglich, eine Person anhand ihrer Browser-Einstellungen zu identifizieren.[101] Fügt man diesen Informationen mit etwas Rechenaufwand den Standort oder die besuchten Websites hinzu, könnte die indirekte Identifizierbarkeit gegeben sein. Das Risiko der Identifizierbarkeit steigt also relativ zum Datenschatz und den zur Verfügung stehenden Rechenressourcen. [102] Entsprechend sind auch „harmlose Details" wie IP-Adressen oder Cookies von der DSGVO geschützt, sofern sie in Kombination mit anderen Daten das Risiko der Identifizierung mit verhältnismäßigem Aufwand darstellen.[103] Handelt es sich nicht um personenbezogene Daten im Sinne der weit gefassten Definition, ist die DSGVO nicht anwendbar. Nicht personenbezogene Daten sind z. B. meteorologische Daten.[104]

Ob anonymisierte, also entpersonalisierte Daten in den Anwendungsbereich fallen, hängt vom angesprochenen relativen Aufwand ab, der für die Re-identifizierung betrieben werden müsste.[105] Die Grenze hin zu identifizierbaren Informationen ist dabei fließend. Ein Datenhändler könnte einen eingekauften, anonymisierten Datensatz mithilfe seines bereits vorhandenen Datensatzes wieder personalisieren und unterläge damit im Gegensatz zum Vorbesitzer der Daten der DSGVO.[106]

vom 19. April 2016, erhältlich im Internet: <https://bit.ly/2TT1hx0> (besucht am 14. Februar *2019); Voigt/Von dem Busche*, EU-Datenschutz Grundverordnung, 293 ff.

96 *Voigt/Von dem Busche*, EU-Datenschutz Grundverordnung, 113.

97 Art. 4 Nr. 1 DSGVO.

98 *Ibid*.

99 Art. 80 Abs. 1 DSGVO.

100 *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (306).

101 *Arning*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 12. Dieses Phänomen wird auch Browser-Fingerprinting genannt. Inwieweit der eigene Browser identifizierbar ist, kann hier getestet werden: <https://panopticlick.eff.org/> (besucht am 19. März 2019).

102 *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (306).

103 Erwägungsgrund Nr. 30 der Verordnung Nr. 2016/679, ABl. EG Nr. L 119/6 vom 27. April 2016.

104 *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (306).

105 *Arning*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 12.

106 *Oostveen*, International Data Privacy Law, Vol. 6 (4), 299 (308); *Voigt/Von dem Busch*e, EU-Datenschutz Grundverordnung, 312.

Wenn personenbezogene Daten verarbeitet werden, muss die Verarbeitung durch einen der sechs Erlaubnistatbestand der DSGVO abgedeckt werden.[107] Ein Beispiel für einen solchen ist die Einwilligung des Betroffenen zur Verarbeitung seiner Daten zum vom Unternehmen angegebenen Verarbeitungszweck gem. Art. 6 Abs. 1 lit. a) DSGVO.

Dabei ist für die Anwendung der DSGVO nicht entscheidend, ob die Verarbeitung in der EU stattfindet, oder ob der Betroffene EU-Bürger ist. Die Anwendbarkeit hängt lediglich davon ab, wo die vertragliche Leistung der Datenverarbeitung angeboten wird. Ist das die EU, gilt die DSGVO. Unabhängig davon, wo sich der eigentliche Sitz des Unternehmens befindet. Die DSGVO entfaltet somit durch das in Art. 3 Abs. 1 DSGVO eingeführte Marktortprinzip extraterritoriale Drittwirkung.[108] Der räumliche und sachliche Anwendungsbereich und dementsprechend weitreichender als die US-Gesetzgebung und könnte hierdurch potenziell in US-Territorium hineinreichen.

Entsprechendes gilt für die Berufung betroffener natürlicher Personen auf die DSGVO sowie für die Rechte und Pflichten der verarbeitenden Unternehmen. Diese gelten im weitreichenden Anwendungsbereich.

Die angesprochenen Pflichten für verantwortliche Datenverarbeiter sind weitreichend. Herausragendes Beispiel hierfür ist die vorgeschriebene Zweckbindung i. V. m. den Datenschutz-Grundsätzen der Datenminimierung und der Transparenzpflicht.[109]

> „Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbaren Weise weiterverarbeitet werden [...]“[110]

Die Datenerhebung und das Ausmaß dieser sind auf einen vorher definierten, dem Betroffenen verständlich zugänglich gemachten Zweck begrenzt. Vorausgesetzt, der Verarbeitung liegt ein Erlaubnistatbestand gem. Art. 6 DSGVO zugrunde. Ändert sich der Zweck, muss die Verarbeitung erneut legitimiert werden. Hierbei muss der Betroffene dem geänderten Zweck gem. Art. 6 Abs. 1 lit. a) DSGVO einwilligen. Dafür gilt, dass das Unternehmen dem Betroffenen die Zwecke gem. Art 13 und 14 DSGVO in verständlicher Weise offenlegen muss, damit dieser freiwillig, informiert und unmissverständlich der Verarbeitung mit einer eindeutig bestätigenden Handlung einwilligen kann.[111]

Die Beweislast liegt hierbei gem. Art. 7 Abs. 1 DSGVO beim verarbeitenden Unternehmen. Die Einwilligung kann der Betroffene gem. Art. 17 DSGVO jederzeit zurückziehen. Die Daten müssen entsprechend gelöscht werden. Kontrolliert werden die Datenverarbeiter dabei von unabhängigen, nationalen Datenschutzbehörden. Der Rechtsweg steht jedem Betroffenen gem. Art. 77 DSGVO offen.

[107] *Voigt/Von dem Busche*, EU-Datenschutz Grundverordnung, 113 ff.
[108] *Ibid*., 27, 31.
[109] Art. 5 Abs. 1 lit. b) DSGVO.
[110] *Ibid.*
[111] Art. 4 Nr. 11 DSGVO; *Voigt/Von dem Busche*, EU-Datenschutz Grundverordnung, 113 ff.

Verstöße gegen die Zweckbindung und andere Pflichten werden mit Strafen von bis zu 4 % des weltweiten Umsatzes geahndet.[112] Die relative Höhe der sog. Verbandsstrafe nutzt das Kosten-Nutzen-Kalkül von Unternehmen aus. Sie treibt die Kosten eines Verstoßes so hoch, dass ein in Kauf genommener Verstoß nicht mehr rational wäre und Technologien aus diesem Grund *a priori* datenschutzfreundlich gestaltet werden.[113] Bei Verstößen sprechen die zuständigen Datenschutzbehörden Strafen aus und verleihen dem europäischen Datenschutz Nachdruck.

Die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) sprach im Januar 2019 eine Strafe von 50 Millionen Euro gegen Google aus. Der Konzern hatte nach Auffassung der Behörde gegen die oben beschriebene Transparenzpflicht bei der Einholung der Einwilligung verstoßen.[114] Als Konsequenz hätten die Einwilligungen der Nutzer nicht in der vorgeschriebenen informierten Art und Weise erfolgen können.[115]

In Verbindung mit dem extraterritorialen Anwendungsbereich mit Drittwirkung kann also festgestellt werden, dass im Gegensatz zur US-Gesetzgebung die DSGVO mit ihren weitreichenden Pflichten für verarbeitende Unternehmen dem Nutzer als Quelle oder – abstrakt formuliert – Eigentümer der Daten eine mächtigere Position einräumt. Der EU-Gesetzgeber verschiebt die im US-Markt beschriebene Informationsasymmetrie auf dem Datenmarkt zu Gunsten des Bürgers als Eigentümer der Daten mit Hilfe der Zweckbindung und den daran angeschlossenen Verbandsstrafen. Der Nutzer wird folglich im Datenmarkt durch die DSGVO ermächtigt.

Diese Einschätzung kann durch die kodifizierten Auskunftsrechte von Betroffenen gegenüber Unternehmen, das Widerspruchsrechte gegen Marketingzwecke, die weitreichenden Rechtsmittel und die oben angesprochenen Strafen bei Verstößen zusätzlich bekräftigt werden.[116] Als Folge könnten sich für Unternehmen, deren Datenverarbeitungen in den Anwendungsbereich fallen, zusätzliche Kosten ergeben, um den zahlreichen Pflichten zu entsprechen.

Allerdings muss einschränkend erwähnt werden, dass das beschriebene Grundrecht auf Datenschutz auch in Europa von mehreren Mitgliedsstaaten mit sicherheitspolitisch begründeten Ausnahmeregelungen beschränkt wird.[117] Ein Beispiel hierfür ist die Vorratsdatenspeicherung.[118] Deren zugrunde liegende Richtlinie erklärte der EuGH für unvereinbar u. a. mit dem in Art. 8 GRCh normierten Grundrecht auf Datenschutz.[119]

[112] Art. 83 Abs. 5lit. a) DSGVO; Gilbert, EU General Data Protection Regulation: What Impact for Businesses Established Outside the EU, vom 19. April 2016, erhältlich im Internet: <https://bit.ly/2TT1hx0> (besucht am 14. Februar 2019).

[113] *Voigt/Von dem Busche*, EU-Datenschutz Grundverordnung, 38 ff.

[114] Einschlägig hierbei sind Art. 6 Abs. 1 lit. a) DSGVO i. V. m. Art. 4 Nr. 11 und Art. 13 DSGVO.

[115] *CNIL*, The CNIL´s restricted committee imposes a financial penalty of 50 Million euros against Google LLC, vom 21. Januar 2019, erhältlich im Internet: <https://bit.ly/2FDztWt> (besucht am 18 Februar 2019).

[116] Recht auf Löschung: Art. 17 DSGVO; Art. 21 und 22 DSGVO; Widerspruchsrechte: Art. 77 i. V. m. Art. 78 DSGVO.

[117] *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (122 f.); *Weichert*, Datenschutz und Datensicherheit, Vol. 12 (2014), 850 (850).

[118] *Herdegen*, Europarecht, § 8, Rn. 28.

[119] *Ibid.*

Hinzu kommen die Öffnungsklauseln der DSGVO für nationalstaatliche Regeln, die das Bild einer einheitlichen, harmonisierten Regelung trüben und bei Normkollisionen die Rechtsunsicherheit für Unternehmen erhöhen könnten.[120]

Die dargestellten Differenzen im Datenschutzrecht können anhand der Ergebnisse als grundlegend bezeichnet werden. Es stehen sich zwei diametral entgegengesetzte Ansätze gegenüber. Inwieweit Privacy Shield als Kompromiss das Verhältnis dieser beiden Ansätze regelt und welche Probleme sich daraus ergeben, wird im folgenden Kapitel untersucht.

IV. Fauler Kompromiss? Privacy Shield

Nachdem der Vorgänger Safe Harbor vom EuGH für ungültig erklärt worden war, wurde das Privacy-Shield-Abkommen zwischen den USA und der zuständigen EU-KOMM verhandelt und im Juli 2016 durch den sog. Angemessenheitsbeschluss der EU-KOMM angenommen.[121] Stand heute wurden 13 Angemessenheitsbeschlüsse zwischen der EU und anderen Ländern beschlossen.[122]

Rechtsgrundlage für den Angemessenheitsbeschluss der EU-KOMM war zum Zeitpunkt der Verhandlungen Art. 25 Abs. 6 der DSLR. Dieser gilt gem. Art. 45 Abs. 9 DSGVO fort. Die Kommission überprüfte demnach, ob die Datenschutzgesetzgebung der USA ein angemessenes Schutzniveau bietet. Ist dem so, wird dies in einem Angemessenheitsbeschluss begründet. Mit der Rechtsfolge, dass die Datenübermittlung in die USA keiner besonderen Genehmigung mehr durch die nationalen Aufsichtsbehörden bedarf, weil das sog. angemessene Schutzniveau erfüllt ist.[123] Der Beschluss hindert die nationalen Datenschutzbehörden aber ausdrücklich nicht daran, Datentransfers anhand des angemessenen Schutzniveaus zu überprüfen und sie ggf. zu unterbinden.[124]

Zum angemessenen Schutzniveau führte der EuGH in seiner Entscheidung zum Vorgängerabkommen aus, dass das Drittland in seiner innerstaatlichen Rechtsordnung oder durch internationale Verpflichtungen ein Schutzniveau gewährleisten muss, „[...] das dem der Union aufgrund der Richtlinie 95/46 im Lichte der Charta garantierten Niveau der Sache nach gleichwertig ist."[125] Das Datenschutzniveau der USA muss also nicht identisch sein, sondern im Gesamtbild und mit den Umständen des Einzelfalls dem der EU angemessen sein.[126] Privacy Shield ist also in diesem Sinne

[120] Beispielhaft: *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 35.
[121] Durchführungsbeschluss der EU-KOMM Nr. 2016/1250, ABl. EG Nr. L 207/1 vom 12. Juli 2016.
[122] *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 26 ff; Japan ist das aktuellste Land, das im Zuge des Freihandelsabkommens JEFTA mit einem Angemessenheitsbeschluss bedacht wurde, vgl. dazu: Angemessenheitsbeschluss der Kommission: Japan ist sicheres Drittland, vom 25. Januar 2019, erhältlich im Internet: <https://www.datenschutzbeauftragter-info.de/angemessenheitsbeschluss-der-kommission-japan-ist-sicheres-drittland/> (besucht am 25. Februar 2019).
[123] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 156 f.
[124] EuGH, Rs. C-362/14, *Schrems vs. Data Protection Commissioner*, Slg. 2015, ECLI:EU:C:2015:650, Rn. 57; 107.
[125] *Ibid*., Rn. 73.
[126] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 156.

eine internationale Verpflichtung der USA, vorbehaltlich derer das Datenschutzniveau der USA der Sache nach für gleichwertig erklärt wurde.[127]

Privacy Shield funktioniert nach dem oben dargestellten US-Prinzip der Selbstzertifizierung. Unternehmen unterwerfen sich freiwillig dem Regime des Privacy Shields. Dies besteht inhaltlich aus sieben Prinzipien und spezifizierenden Sonderprinzipien, deren Einhaltung vom US-Handelsministerium u. a. mit Stichproben überwacht wird.[128] Zusätzlich gibt es FAQs und Guidelines für Unternehmen, um diesen die Einhaltung zu erleichtern.[129] Selbstzertifizierte Unternehmen werden vom US-Handelsministerium auf einer online einsehbaren Liste geführt. Die Unternehmen müssen sich jährlich neu zertifizieren, also aktiv beim US-Handelsministerium melden. Passiert dies nicht, führt dies zum Ausschluss. Ausgeschlossene Unternehmen werden auf einer Negativliste geführt, die ebenfalls einzusehen ist. Nicht zertifizierte Unternehmen dürfen keine Daten aus der EU übermitteln.[130] Derzeit sind 4.442 Unternehmen positiv und 315 negativ gelistet.[131]

Inhaltlich problematisch könnte das Privacy-Shield-Abkommen sein, weil sich der oben dargestellte Maßstab des Datenschutzes durch die DSGVO gegenüber den USA erheblich verändert hat. Der Angemessenheitsbeschluss basiert jedoch auf dem Vorgänger der DSGVO, der DSLR. Der Beschluss und Privacy Shield müssen sich aber an dem oben dargestellten, weiter entwickelten Datenschutzniveau der DSGVO und vom EuGH festgelegten Maßstäben messen lassen und diese zumindest der Sache nach erfüllen.[132] Zu diesem gehören insbesondere die am Vorgänger-Abkommen bemängelten unabhängige Datenschutzbehörden, internationale Verpflichtungen sowie materielle Datenschutzregelungen und Rechtsmittel.[133]

Dieser Kritik sollte der Privacy Shield mit Verbesserungen in allen drei Bereichen begegnen. Als Ergebnis sollte ein rechtssicheres Regime für den Datentransfer zwischen der EU und den USA entstehen und ein Rechtsvakuum wie nach der *Schrems*-Entscheidung verhindert werden. Um dies zu garantieren, überprüft die EU-KOMM jährlich die Umsetzung der angekündigten Verbesserungen und damit die Gültigkeit der auf Privacy Shield basierten Angemessenheitsentscheidung.[134] Inwieweit dies gelungen ist, wird im Folgenden diskutiert.

[127] *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 34 f.

[128] *EU-KOMM*, Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, 2 f., vom 19. Dezember 2018, erhältlich im Internet: <https://bit.ly/2BvTud2> (besucht am 18. März 2019).

[129] *U.S. Department of Commerce*, FAQs - General, erhältlich im Internet: <https://bit.ly/2FgOLxK> (besucht am 20. Februar 2019).

[130] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 163. Einschränkend muss angemerkt werden, dass die Übertragung rechtens sein kann, sofern geeignete Garantie gem. Art. 46 oder Ausnahmeregelung gem. Art. 49 DSGVO bestehen.

[131] *U.S. Department of Commerce*, Privacy Shield List, erhältlich im Internet: <https://www.privacyshield.gov/list> (besucht am 19. Februar 2019).

[132] *Voss*, Journal of Internet Law, Vol. 19, No. 11 (2016), 1; 9 (16).

[133] Art. 45 Abs. 2 DSGVO; EuGH, Rs C-362/14 *Schrems vs. Data Protection Commissioner*, Slg. 2015, ECLI:EU:C:2015:650, Rn. 62; *Moos/Zeiter*, in Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 45 ff.

[134] Beispielhaft *EU-KOMM*, Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, vom

Um den im Vorgängerabkommen bemängelten, weil fehlenden Rechtsmitteln für EU-Bürger bei Datenschutzverstößen zu begegnen, wurde im US-Recht der Privacy Act mit dem Judicial Redress Act reformiert. Dies bemerkte auch die EU-KOMM in ihrer ersten Überprüfung positiv.[135] Die zur Verfügung stehenden Rechtsmittel im Judicial Redress Act sind dabei jedoch, wie oben dargelegt, sehr begrenzt und nicht mit der unmittelbaren und extraterritorialen Anwendbarkeit der DSGVO vergleichbar.[136]

Weiterhin müssen sich Unternehmen mit dem Privacy Shield einem selbstgewählten, bindenden Streitschlichtungsverfahren unterwerfen.[137] Dies wird insofern kritisiert, dass Betroffenen der Zugang zur Streitschlichtung durch zusätzliche Hürden erschwert werde. Dazu gehören u. a. die notwendigen Bedingungen für das Streitschlichtungsverfahren. Betroffene müssen sich unter Berufung auf Privacy Shield erfolglos an das jeweilige Unternehmen gewandt haben. Zusätzlich muss der Fall durch die Europäische Datenschutzbehörde beim zuständigen US-Handelsministerium bemerkt worden sein.[138] Es besteht demzufolge ein wesentlicher Unterschied zwischen der festgestellten extraterritorialen, unmittelbaren Anwendbarkeit der DSGVO für Betroffene und dem an Bedingungen geknüpften, privaten Streitschlichtungsverfahren.

Hierbei muss die Einschränkung gemacht werden, dass auch private Streitschlichtungsverfahren einen bindenden Schiedsspruch in der Sache produzieren würden. Einschlägiges US-Recht hierzu ist der Federal Arbitration Act.[139] Die Zustimmung der Unternehmen zu einem Verfahren und die Hürden des Zugangs sind jedoch ein substantieller Unterschied zur öffentlichen Gerichtsbarkeit in der EU.[140]

Um den im Vorgänger-Abkommen fehlenden unabhängigen Aufsichtsmechanismen entgegenzukommen, wurde die Position einer Ombudsperson beim US-Außenministerium eingerichtet.[141] Dies wurde grundsätzlich von der EU-KOMM und anderen Stellen begrüßt.[142]

Jedoch erscheint die Angliederung an das US-Außenministerium problematisch. Die Funktion einer unabhängigen Aufsicht könnte durch die Angliederung und der damit einhergehenden Dienstaufsicht bzw. Weisungsgebundenheit *ad absurdum* geführt werden. Zusätzlich widerspricht dies der europäischen Vorstellung des oben

19. Dezember 2018, erhältlich im Internet: <https://bit.ly/2BvTud2> (besucht am 18. März 2019).

135 *Ibid*., 4.

136 *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 129.

137 *U.S. Department of Commerce*, Privacy Shield Framework, 33-36, erhältlich im Internet: <https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text> besucht am 25. März 2019).

138 *Weichert*, Privacy Shield, 12 ff.

139 *U.S. Department of Commerce*, Privacy Shield Framework, 34.

140 *Weichert*, Privacy Shield, 14.

141 *U.S. Department of State*, Privacy Shield Ombudsperson, erhältlich im Internet: <https://www.state.gov/e/privacyshield/ombud/> (besucht am 19. März 2019); *U.S. Department of Commerce*, Privacy Shield Attachment A, erhältlich im Internet: <https://www.privacyshield.gov/ps-ftc-letter-attachment-a>(besucht am 21. Februar 2019).

142 *EU-KOMM*, Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, vom 19. Dezember 2018, 4; *Schrems,* Privacy Shield – Press Breakfast with Jan Albrecht, 2.

angeführten Art. 8 Abs. 3 GRCh, sowie der Rechtsprechung des EUGH zum Vorgänger-Abkommen.[143]

Zusätzlich ist die bis heute fehlende permanente Besetzung der Position ein Problem hinsichtlich der Effektivität der auszuübenden Aufsicht. Diese kann u. a. von einer kontinuierlichen personellen Besetzung abhängen. Auch die EU-KOMM bemängelt diesen Sachverhalt.[144]

Des Weiteren besteht der Zugang zu Ombudsperson für Betroffene nur indirekt. Ein EU-Bürger muss sich mit seiner Beschwerde erst an die nationale Datenschutzbehörde in der EU wenden. US-Unternehmen betreffende Beschwerden werden danach von diesen an eine EU-Beschwerdeannahmestelle herangetragen, gesammelt und an die US-Ombudsperson weitergegeben. Die Ombudsperson informiert nach Eingang über Status und Verlauf des Verfahrens. Dabei verständigt die Ombudsperson die Sammelstelle der EU darüber, dass es entweder keinen Verstoß gegen das oben beschriebene Recht gab oder, bei einem Verstoß, dieser behoben wurde. Über Umfang, Art des Verstoßes und ggf. eingeleitete Maßnahmen wird ausdrücklich nicht informiert.[145]

Inwiefern mit der Ombudsperson also eine unabhängige und effektive Anlaufstelle entstanden ist, deren Zugang der Sache nach gleichwertig zur unmittelbaren Anwendbarkeit im EU-Recht ist, kann durchaus in Frage gestellt werden.

Als weiteres Aufsichtsgremium kontrolliert das Privacy and Civil Liberties Oversight Board (PCLOB) die US-Geheimdienste. Die Funktion betrifft insofern auch den Datenschutz von EU-Bürgern.[146] Das PCLOB war bis Oktober 2018 nicht ausreichend besetzt und erfüllte das für seine Funktion notwendige Quorum nicht. Entsprechend fiel dieses Gremium für zwei Jahre des Abkommens aus.[147] Inwiefern heute hierin eine unabhängige Aufsichtsfunktion besteht, wird die dritte Überprüfung der EU-KOMM im Jahr 2019 zeigen müssen.

Zusammengefasst kann festgehalten werden, dass Privacy Shield hinsichtlich der geforderten unabhängigen Aufsichtsbehörden und zugänglichen Rechtsmittel problematisch ist. Zu indirekt erscheint der Weg über die Schiedsgerichtsbarkeit, zu abhängig, personell und kompetenziell unterausgestattet erscheinen die installierten Auf-

[143] *Weichert*, Privacy Shield, 15; EuGH, Rs. C-362/14, *Schrems vs. Data Protection Commissioner*, Slg. 2015, ECLI:EU:C:2015:650, Rn. 62.

[144] *EU-KOMM*, Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, 4.

[145] *U.S. Department of Commerce*, Privacy Shield Attachment A, o.A.; *U.S. Department of Commerce*, Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, 3 ff., erhältlich im Internet: <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g> (besucht am 21. Februar 2019); *European Parliamentary Research Service (EPRS)*, The Privacy Shield, Update on the state of play of the EU-US data transfer rules, 19-22, vom Juli 2018, erhältlich im Internet: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf> (besucht am 19. März 2019).

[146] *EPRS*, The Privacy Shield, Update on the state of play of the EU-US data transfer rules, 20, vom Juli 2018, erhältlich im Internet: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf> (besucht am 19. März 2019).

[147] *EU-KOMM*, Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, vom 19. Dezember 2018, 4.

sichtsmechanismen. Einschränkend muss der Judicial Redress Act erwähnt werden, der EU-Bürgern Rechtsmittel ermöglicht. Diese werden aber als sehr eingeschränkt beschrieben. Käme es zu einer Überprüfung der Angemessenheitsentscheidung durch den EuGH, könnte er diese aufgrund der oben beschriebenen Sachverhalte für ungültig erklären. Entsprechend kritisierte die Artikel-29 Datenschutzgruppe der EU das Privacy-Shield-Abkommen als unzureichend für Unternehmen und Betroffene.[148]

Vergleicht man die sieben Prinzipien des Privacy Shields inhaltlich mit den oben beschriebenen Grundsätzen der DSGVO, fällt grundsätzlich die Diskrepanz in Reichweite und Bindung der beiden Regelungen auf. Diese ist beim Privacy Shield zunächst der Sache nach geringer, weil das Abkommen lediglich ein Regime für den Datentransfer darstellt, keine Grundverordnung ist und diese nur ergänzen kann. Die sieben Prinzipien sind dabei inhaltlich an die DSGVO angelehnt. [149] Beispielsweise soll an dieser Stelle das erste Prinzip, das sog. Notice-Prinzip, besprochen werde.

Angelehnt an die Transparenz- und Informationspflichten der DSGVO schreibt Privacy Shield US-Unternehmen vor, Informationen über die Verpflichtung zum Privacy Shield, die gewählte Streitbeilegungsmöglichkeit, bestehende Auskunftsrechte beim Unternehmen oder Aufsichtsbehörden und Informationen über Zweck und Art der Datenverarbeitung sowie eventuell involvierte Auftragsverarbeiter zur Verfügung zu stellen.[150] Unter diesen Bedingungen und i. V. m. den anderen Prinzipien gilt die Datenverarbeitung *a priori* als legal.[151] Die Vorschriften selbst sind den Transparenz- und Informationspflichten gem. Art. 12 und 13 DSGVO ähnlich. Im Gegensatz dazu gilt in der DSGVO, dass die Erhebung personenbezogener Daten *a priori* illegal ist und nur durch einen Erlaubnistatbestand gerechtfertigt werden kann.[152]

Weiterhin sieht Privacy Shield keine Strafen bei Verstößen vor.[153] Dadurch kann die Wirksamkeit im Gegensatz zum Maßstab DSGVO durchaus hinterfragt werden, da abgesehen vom öffentlichen Vertrauensschaden im Falle einer Überprüfung keine monetäre Strafe die Kosten des Verstoßes erhöhen. Den Informations- und Transparenzpflichten wird also kein Nachdruck verliehen.

Problematisch könnte weiterhin sein, dass für die Interpretation der inhaltlichen Prinzipien US-Recht gilt: [154]

> „U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have com-

[148] *Article 29 Data Protection Working Party (WP29)*, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 4 f., vom 13. April 2016, erhältlich im Internet: <https://bit.ly/2Fc2S7H> (besucht am 18. März 2019).

[149] *Zeni/Gilbert/Calehuff*, GDPR and Privacy Shield: Different Tools for Different Goals, vom 26. November 2018, erhältlich im Internet: <https://www.francoisegilbert.com/?m=201811> (besucht am 21. Februar 2019).

[150] *U.S. Department of Commerce*, EU-U.S. Privacy Shield Framework, 4 f.

[151] *Zeni/Gilbert/Calehuff*, GDPR and Privacy Shield: Different Tools for Different Goals, vom 26. November 2018, erhältlich im Internet: <https://www.francoisegilbert.com/?m=201811> (besucht am 21. Februar 2019).

[152] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 113.

[153] *Zeni/Gilbert/Calehuff*, GDPR and Privacy Shield: Different Tools for Different Goals, vom 26. November 2018, erhältlich im Internet: <https://www.francoisegilbert.com/?m=201811> (besucht am 21. Februar 2019).

[154] *Bender*, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117 (132).

mitted to cooperate with European data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant."[155]

Dies könnte zunächst dazu führen, dass die im Unterkapitel III beschriebenen, engen Definitionen der Datenverarbeitung zur Anwendung kommen. Diese widersprechen dem breit angelegten Schutzbereich sowie der Ratio der DSGVO. Hinzu kommt, dass damit die besprochenen, geheimdienstlichen Befugnisse der EO12333, der PPD-28 und des FISA im Sinne der nationalen Sicherheit vorgehen könnten.[156] Dass dies der EuGH wie in der *Schrems*-Entscheidung erneut bemängeln könnte, erscheint möglich.

Gem. Art. 44 i. V. m. Art. 45 Abs. 1 DSGVO gilt, dass, ungeachtet des Angemessenheitsbeschlusses, Unternehmen und deren Datenverarbeitungen in Drittländer auch alle sonstigen, im vorangegangenen Kapitel beschriebenen Vorschriften der DSGVO einhalten müssen.[157] Effektiv müssten Datentransfers unter Privacy Shield den weitreichenderen, extraterritorial geltenden Vorschriften der DSGVO standhalten. Was sie nicht leisten können, wenn sich die verarbeitenden Unternehmen nach den dargestellten Privacy-Shield-Prinzipien richten. Im Ergebnis könnte Rechtsunsicherheit bei Betroffenen und Unternehmen bestehen, nach welcher der hier kollidierenden Vorschriften sie sich richten sollen. Zieht man die oben festgestellten Problematiken hinsichtlich der unabhängigen Aufsichtsbehörden sowie der Rechtsmittel hinzu, könnte die Rechtssicherheit von Privacy Shield und damit die der Angemessenheitsentscheidung für die USA angezweifelt werden.

Wäre die Angemessenheitsentscheidung ungültig, wäre damit die Rechtsgrundlage für die Datenübermittlungen zwischen der EU und den USA nicht gegeben und als Resultat *de jure* nicht möglich, sofern keine alternativen Regelungen bestehen. Entsprechende Verfahren zur Überprüfung der Angemessenheitsentscheidung sind seit September 2016 anhängig und könnten ein ähnliches Rechtsvakuum wie nach der *Schrems*-Entscheidung auslösen.[158] Die Folgen wären für die 4.442 gelisteten Unternehmen und betroffene Personen erheblich.

Welche Probleme die oben dargestellte Rechtskollision und die bestehende Rechtsunsicherheit in den praktischen Bereichen Cloud-Computing, Big Data und E-Discovery darstellen könnten und welche Empfehlungen sich daraus ableiten lassen, wird im nächsten Kapitel diskutiert.

155 *U.S. Department of Commerce*, EU-U.S. Privacy Shield Framework, 3.
156 *Weichert*, Privacy Shield, 12.
157 *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 156 f.
158 *Moos/Zeiter*, in Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 43.

D. Realität vs. Regulierung: Cloud-Computing, Big Data und E-Discovery

I. Cloud-Computing

Cloud-Computing wird vom IT-Branchenverband BITKOM definiert als

> „[...] eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet. Damit ermöglicht Cloud-Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand."[159]

Beim Cloud-Computing ist es, abgeleitet von der Definition, systemimmanent, dass Daten über Grenzen hinweg verteilt werden und die Verarbeitung oder der Zugriff auf diese Daten dezentral und parallel stattfindet. Um den schnellen Zugriff von Kunden und Betroffenen auf Daten von jedem Punkt aus sicherzustellen, wird der nächstgelegenste Server mit freier Rechenkapazität angesteuert.[160]

Dies geschieht über Grenzen hinweg global und wird von Unternehmen wie privaten Kunden genutzt. 2016 nutzten 38 % der Unternehmen in Deutschland mit 250 oder mehr Beschäftigten Cloud-Dienste.[161] Entsprechend sind Anbieter dieser Dienste von der DSGVO und Privacy Shield gleichermaßen betroffen, wenn personenbezogene Daten zwischen der EU und den USA übermittelt werden.[162]

Entscheidend für den Anwendungsbereich beider Regime ist dabei, ob Cloud-Computing-Anbieter wie das amerikanische Unternehmen IBM personenbezogene Daten von natürlichen Personen im Gesetzsinne verarbeiten.[163] Ist dies der Fall, muss das US-Unternehmen Privacy Shield einhalten, um von der beschriebenen Angemessenheitsentscheidung der EU-KOMM zu profitieren. Bei IBM ist das der Fall.[164]

Damit erfüllt das Unternehmen aber nur eine Anforderung für den Datentransfer von Drittländern gemäß DSGVO.[165] Wie oben dargestellt, gilt die DSGVO nach dem Marktortprinzip extraterritorial.[166] Das heißt, dass das verarbeitende Unternehmen aus den USA nicht nur an Privacy Shield, sondern gem. Art. 44 DSGVO auch

[159] *BITKOM*, Cloud-Computing, 14.
[160] *Ibid.*, 20-23.
[161] *Brandt*, So viele Unternehmen zahlen für die Cloud, vom 01. September 2017, erhältlich im Internet: <https://de.statista.com/infografik/10923/cloud-computing-nutzung-von-unternehmen-in-deutschland/> (besucht am 26. Februar 2019).
[162] *Heinemann/Meyerdierks*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 127-132.
[163] Art. 4 Nr. 1 DSGVO; vgl. für Marktführer-Aussage: *Statista GmbH*, Cloud-Computing Dossier, 12.
[164] *U.S. Department of State*, International Business Machines Cooperation, erhältlich im Internet: <https://www.privacyshield.gov/participant?id=a2zt0000000TOAoAAO&status=Active> (besucht am 26. Februar 2019).
[165] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 156 ff.; Art. 44 und Art. 45 DSGVO.
[166] Art. 3 Abs. 1 DSGVO.

an die in Kapitel C. III. dargestellten Regelungen, also auch an „die sonstigen Bestimmungen dieser Verordnung [...]“ gebunden sind.[167]

Dies ist besonders relevant, wenn US- und EU-Cloud-Unternehmen Rechen- und Speicherkapazität in anderen Drittländern von Drittunternehmen anmieten, um ihren Service weltweit kosteneffizient anbieten zu können. Rechtlich wird dabei von dem verantwortlichen Unternehmen, dem Verantwortlichen, die Dienstleistung an einen sog. Auftragsverarbeiter delegiert.[168]

Werden von einem US-Cloud-Anbieter hierbei in der EU erhobene, personenbezogene Daten an einen Cloud-Anbieter – dem Auftragsverarbeiter – in einem Drittland übermittelt, ist durch das Marktortprinzip der Anwendungsbereich der DSGVO eröffnet. Damit gelten die einschlägigen Vorschriften für Datenübermittlungen in Drittländer in Art. 44 bis 49 DSGVO sowie alle anderen Vorschriften der DSGVO.[169] Dies gilt entsprechend auch bei Auftragsverarbeitungen in Regionen und Ländern mit vergleichsweise schwachem Datenschutz wie Afrika, Russland sowie Mittel- und Südamerika.[170]

Für die Cloud-Anbieter als Verantwortliche i. S. d. Gesetzes entstehen hierbei unterschiedlich weitreichende Pflichten. Privacy Shield sieht im Notice-Prinzip vor, dass der Cloud-Anbieter den Betroffenen über Drittparteien informiert, die unter dem angegeben Zweck Auftragsverarbeitungen vornehmen. Bei einer Abweichung vom eigentlichen Zweck sieht das Abkommen eine Benachrichtigung des Betroffenen – bei Zweckentfremdung sensibler Daten eine aktive Zustimmung des Betroffenen vor. Des Weiteren verpflichtet sich der Auftragsverarbeiter gegenüber dem Verantwortlichen vertraglich, Privacy Shield einzuhalten und den Verantwortlichen zu unterrichten, falls die Einhaltung des Abkommens nicht mehr möglich ist. Für Sicherheitsprobleme während der Auftragsverarbeitungen enthält Privacy Shield keine Vorschrift.[171]

Die DSGVO geht hierbei wesentlich weiter. Die in Kapitel C. III. dargestellten Transparenz- und Informationspflichten sowie die Strafen bei Zuwiderhandlung gelten für die gesamte Verarbeitungskette. Sie gelten entsprechend auch für den Auftragsverarbeiter und dessen Auftraggeber, dem Verantwortlichen i. S. d. Gesetzes[172]

Gem. Art. 28 Abs. 3 DSGVO verpflichtet sich der Auftragsverarbeiter gegenüber dem Verantwortlichen vertraglich zur Einhaltung der DSGVO. Um die allgemeinen Pflichten wie das Recht auf Vergessen auf Antrag des Betroffenen sicherzustellen, muss der Vertrag zwischen Cloud-Anbieter und Auftragsverarbeiter dem Umstand Rechnung tragen, dass die Durchführung einer Datenlöschung und deren Nachweisbarkeit in einer Cloud-Umgebung über Länder- und Servergrenzen hinweg Schwierigkeiten bergen. Entsprechend muss der Vertrag die Bedingungen der Löschung näher beschreiben, um diese sicherzustellen. Ist das nicht gewährleistet, drohen bei einer

167 *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 156.
168 *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (10 f).
169 *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 27.
170 *Roos*, Westliche Länder haben beim Datenschutz die Nase vorn, vom 13. März 2014, erhältlich im Internet: <https://www.heise.de/ix/meldung/Westliche-Laender-haben-beim-Datenschutz-die-Nase-vorn-2169187.html> (besucht am 26. Februar 2019).
171 *Zeni/Gilbert/Calehuff*, GDPR and Privacy Shield: Different Tools for Different Goals, vom 26. November 2018.
172 Art. 28 Abs. 1 und 2 DSGVO.

Überprüfung im schlimmsten Fall die beschriebenen Verbandsstrafen bzw. ein Übermittlungsverbot.[173]

Auftragsverarbeiter innerhalb der EU genießen hierbei insofern eine privilegierte Stellung, dass es bei ihrer Einbeziehung durch Cloud-Anbieter keiner zusätzlichen Einwilligung des Betroffenen bedarf.[174] Wollen wiederum Auftragsverarbeiter weitere Subunternehmer beauftragen, muss gem. Art. 28 Abs. 2 DSGVO die Genehmigung des verantwortlichen Cloud-Anbieters vorliegen. Über jede weitere Hinzuziehung muss der Auftragsverarbeiter den Verantwortlichen informieren, da dieser ein Widerspruchsrecht hat. Der Subunternehmer unterliegt hierbei denselben Pflichten wie Verantwortliche und Auftragsverarbeiter vor ihm.[175]

Für Auftragsverarbeiter aus Drittländern gelten die oben dargestellten Schranken. Erstens muss die Datenübermittlung einem Erlaubnistatbestand gem. Art. 6 DSGVO i. V. m. Art. 44 DSGVO unterliegen. Soweit ist dies äquivalent zu EU-Auftragsverarbeitern. Zweitens muss es gem. Art. 45 Abs. 3 DSGVO einen Angemessenheitsbeschluss mit dem jeweiligen Drittland des Auftragsverarbeiters geben. Ist dem so, stellt die Übermittlung vorbehaltlich der Einhaltung der DSGVO-Pflichten kein Problem dar.[176]

Ist das nicht der Fall, kann die Datenübertragung von Cloud-Anbietern grundsätzlich nur aufgrund sog. geeigneter Garantien gem. Art. 46 DSGVO oder auf Basis einer Ausnahme im Einzelfall gem. Art. 49 DSGVO erfolgen. Diese sollen den fehlenden Angemessenheitsbeschluss kompensieren und so den effektiven Datenschutz in Ländern ohne angemessenen Datenschutz garantieren.[177]

Nimmt man die festgestellte Rechtsunsicherheit von Privacy Shield aus dem vorherigen Kapitel hinzu, könnte die Praktikabilität des Abkommens abgesehen von seiner sekundärrechtlichen Notwendigkeit hinterfragt werden. Die Vorschriften des Privacy Shield werden durch das Marktortprinzip für betroffene Cloud-Anbieter *ad absurdum* geführt. Sie müssen die Vorschriften der DSGVO einhalten, um personenbezogene Daten verarbeiten zu dürfen.

Dass die DSGVO-Konformität von Cloud-Anbietern u. a. dadurch zu einem wichtigen Entscheidungskriterium für die Auswahl des Cloud-Anbieters geworden ist, erscheint nachvollziehbar. So könnte die DSGVO-Konformität und der damit verbundene Datenschutz zu einem Standortvorteil für europäische Cloud-Anbieter werden, der bei steigender Sensibilität und Nachfrage für das Thema Datenschutz nicht zu unterschätzen ist. Als Reaktion bietet z. B. Microsoft ab Ende 2019 einen Cloud-Dienst „[...] mit besonders strengen Datenschutz- und Compliance-Richtlinien in Deutschland, der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) [...] "[178] an.

[173] *Meyerdierks*, in: Moos et al. (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 137 f.
[174] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 103.
[175] *Ibid*., 108.
[176] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 156 f.; *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), DSGVO Kommentar, Kapitel 9, Rn. 17.
[177] *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn 49. ff.
[178] *Microsoft*, Microsoft stellt Cloud-Dienste ab Ende 2019 aus neuen Rechenzentren in Deutschland bereit und reagiert damit auf veränderte Kundenanforderungen, erhältlich im Internet:

Im Ergebnis fasst die Datenschutzexpertin *Francoise Gilbert* zusammen:

> „Some organizations assume that it is enough for them to have self-certified their adherence to the EU-US Privacy Shield (Privacy Shield) and that their self-certification is sufficient to address all 99 articles of the GDPR. This is incorrect."[179]

Im Ergebnis empfiehlt es sich für Cloud-Anbieter im transatlantischen Verhältnis also nicht nur, sich an die Vorgaben der DSGVO zu halten. Aufgrund der unsicheren Zukunft von Privacy Shield könnte es sinnvoll sein, sich den geeigneten Garantien der DSGVO zu unterwerfen. So könnte einerseits dem Datenschutz Rechnung getragen und andererseits ein eventueller Wettbewerbsvorteil als sog. First Mover generiert werden. Inwieweit die geeigneten Garantien als Alternativen sinnvoll sind, wird in Kapitel E diskutiert.

II. Big Data

Der archetypische Verarbeitungsvorgang im Bereich von Big Data zeigt die (fließenden) Grenzen des Anwendungsbereichs von Datenschutzgesetzen. Big Data wird vom Wissenschaftlichen Dienst des Bundestages definiert als

> „[...] ein Bündel neu entwickelter Methoden und Technologien, die die Erfassung Speicherung und Analyse eines großen und beliebig erweiterbaren Volumens unterschiedlich strukturierter Daten ermöglicht."[180]

Die Technologie charakterisiert sich also u. a. dadurch, große Volumina unterschiedlichster Daten in hoher Geschwindigkeit zu verarbeiten.[181]

Anders als z. B. in wissenschaftlichen Studien werden dabei keine Hypothesen getestet. Die Daten werden nicht mit einem vorher definierten Zweck erhoben. Ziel ist es, aus Kombinationen und statistischer Korrelation verschiedenster Daten Hypothesen zu bilden, deren Wahrscheinlichkeit Anlass für weitere Analysen ist. Je mehr Daten, desto mehr Möglichkeiten können getestet werden; desto valider und reliabler sind die Korrelationen. Im Ergebnis widerspricht das Prinzip von Big Data der Zweckbindung von DSGVO und Privacy Shield.[182]

Abgesehen davon kommen im Bereich Big Data die unterschiedlich weit ausgelegten Anwendungsbereiche der DSGVO und Privacy Shield zum Tragen. Wie bereits in Kapitel C. III. festgestellt, lässt Privacy Shield mit den amerikanischen Begriffen als Interpretationsgrundlage grundsätzlich mehr Datenverarbeitung abseits der Regulie-

<https://products.office.com/de-de/office-365-deutschland/office-365-deutschland> (besucht am 26. Februar 2019).

179 *Zeni/Gilbert/Calehuff*, GDPR and Privacy Shield: Different Tools for Different Goals, vom 26. November 2018.

180 *Wissenschaftlicher Dienst des Bundestages*, Big Data, 1.

181 In der Literatur wird hierbei von den sog. drei Vs gesprochen. Volume (Menge der Daten), Velocity (Geschwindigkeit) und Variety (Vielfalt der Datenquellen- und arten). Vgl. dafür *ibid.*, sowie *Meyerdierks*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 143.

182 *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (301 f.).

rung zu. Bei Zweckentfremdung durch Dritte sieht aber auch Privacy Shield eine Benachrichtigung und die aktive Zustimmung des Betroffenen vor.[183]

Dies gilt aber äquivalent zur DSGVO nur, wenn es sich überhaupt um personenbezogene Daten im Gesetzessinne handelt. Big-Data-Unternehmen bestreiten dies, da der Anwendungsbereich die besprochenen Rechtspflichten von Privacy Shield und DSGVO zur Folge hätte.[184]

Interessant und problematisch zugleich ist hieran, dass am Verarbeitungsprozess von Big Data die Grenzen des personenbezogenen Datums im Gesetzessinn und damit die des Anwendungsbereichs verschwimmen. Wie in Kapitel C. III. besprochen, handelt es sich bei personenbezogenen Daten gem. DSGVO um Informationen, die mittelbar oder unmittelbar zur Identifikation einer Person beitragen können. Dies gilt relativ. Das heißt, dass Daten, die mit erheblichen Aufwand trotz Pseudonymisierung oder Anonymisierung zur Identifikation beitragen können, geschützt sind, sofern dem jeweiligen Verarbeiter die Mittel für die Repersonalisierung zur Verfügung stehen.[185] Die Grenze des Anwendungsbereichs der DSGVO ist entsprechend fließend und aus diesem Grund für Big-Data-Unternehmen besonders relevant.

Anonymisiert ein Datenhändler erhobene Daten, sodass sie für ihn und für andere nur mit unverhältnismäßigem Aufwand wieder personalisiert werden könnten, gilt die DSGVO womöglich nicht.[186] Kauft ein Big-Data-Unternehmen diesen Datensatz und verbindet diese in einer ersten Phase der Verarbeitung mit seinen Rechenressourcen, könnte die Identifizierung relativ zu den zur Verfügung stehenden Ressourcen wieder möglich, der Schutzbereich also eröffnet sein. Typischer Weise randomisieren Big-Data-Unternehmen in einem zweiten Schritt ihre Daten. Dies ist die sog. Analysephase. Sie arbeiten in dieser Phase induktiv: Sie leiten aus einer möglichst großen Anzahl einzelner Datensätze statistische Zusammenhänge für die Allgemeinheit ab. In dieser Phase wäre die DSGVO also wohlmöglich wieder nicht anwendbar, weil die Identifizierung durch Anonymisierung durch den Verarbeiter selbst oder Dritte nicht mehr möglich ist. In einer dritten, der sog. Anwendungsphase, werden diese Erkenntnisse z. B. von Versicherungen deduktiv benutzt. Die allgemeinen Erkenntnisse der Daten haben in dieser Phase potenziell Einfluss auf Einzelschicksale. Der Einzelne wird dabei nicht identifiziert, aber abgeglichen. Dazu müssten seine personenbezogenen Daten mit den Ergebnissen verglichen werden. Die Allgemeinen Erkenntnisse könnten den Betroffenen im Ergebnis in seiner informationellen Selbstbestimmung beeinflussen. Damit könnte der Anwendungsbereich wiedereröffnet sein.[187]

Wäre dem so, sind für Big-Data-Unternehmen Art. 30 und 35 DSGVO relevant. Die einzelnen Verarbeitungsschritte der Daten müssen hiernach u. a. mit dem zugehören Verarbeitungszweck elektronisch aufgezeichnet und auf Verlangen der europäi-

[183] *U.S. Department of Commerce*, EU-U.S. Privacy Shield Framework, 3.
[184] *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (308); an dieser Stelle kann angemerkt werden, dass die im Anwendungsbereich der DSGVO geltenden Transparenz-und Informationspflichten dem Geschäftsmodell der als undurchsichtig geltenden Industrie zuwiderlaufen, vgl. dazu *ibid.*; *Arning*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 19.
[185] *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (306).
[186] *Ibid.*
[187] *Ibid.*, 306 ff.

schen Datenschutzbehörden herausgegeben werden.[188] Die Beweislast trägt das Unternehmen.[189]

Des Weiteren ist ggf. ein sog. Data Protection Impact Assessment (DPIA) vorzunehmen. In dieser müssen die Datenverarbeiter ihre Verarbeitungsverfahren beschreiben, die Notwendigkeit und Verhältnismäßigkeit dieser gegenüber dem angegeben Zweck bewerten und die bestehenden Risiken für Betroffene analysieren. Je nach Risiko für die informationelle Selbstbestimmung von Betroffenen sind adäquate Maßnahmen zu ergreifen, um dieses zu minimieren.[190] Das Verfahren ist zu dokumentieren.[191]

Hierbei bestehen in der Literatur Zweifel, ob das DPIA grundsätzlich durchzuführen ist.[192] Die Artikel-29-Datenschutzgruppe bestätigte diese Zweifel und entwickelte einen Kriterienkatalog mit insgesamt neun Kriterien zur Klärung der Pflichtfrage.[193] Dem Katalog zu Folge wird die DPIA empfohlen, wenn die Datenverarbeitung mehr als zwei der aufgestellten Kriterien betrifft.[194] Zu diesen gehören u. a. die für Big Data typischen automatischen Entscheidungsfindungen und in großen Umfang verarbeitete Daten.[195]

Des Weiteren müssen die nationalen Datenschutzbehörden sog. Backlists erstellen. In diesen werden Verarbeitungsvorgänge geführt, für die ein DPIA zwingend ist.[196] Beispielhaft führt der hessische Datenschutzbeauftrage in seiner Liste unter Punkt acht das „Zusammenführen von personenbezogenen Daten aus verschiedenen Quellen [...] mit dem Beispiel von Big-Data-Analysen an.[197] Folglich sind DPIAs im Anwendungsbereich der DSGVO für Big-Data-Unternehmen – vorbehaltlich der gesetzlichen Ausnahmen – als obligatorisch einzuschätzen.[198]

Im Ergebnis kann anhand dieses Beispiels gezeigt werden, dass die Grenzen der Identifizierbarkeit als Demarkationslinie des Datenschutzes fließend sind.[199] Zieht

[188] Art. 30 Abs. 1 DSGVO.
[189] Art. 7 Abs. 1 DSGVO.
[190] Art. 35 Abs. 1 DSGVO.
[191] Gardyan-Eisenlohr/Cornelius, in: Moos/Schefzig/Arning (Hrsg), Die neue Daten-schutz-Grundverordnung, Kapitel 12, Rn. 77 ff.
[192] *Ibid*., Rn. 69.
[193] *WP 29*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA), 10 ff.
[194] *Ibid*., 12.
[195] *Gardyan-Eisenlohr/Cornelius*, in: Moos/Schefzig/Arning (Hrsg): Die neue Datenschutz-Grundverordnung, Kapitel 12, Rn. 72 ff.
[196] Art. 35 Abs. 4 DSGVO.
[197] *Hessischer Datenschutzbeauftragter*, Liste der Verarbeitungsmöglichkeiten nach Art. 35 Abs. 4 DS-GVO für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen durchzuführen ist, vom August 2018, erhältlich im Internet: <https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_Verarbeitungsvorg%C3%A4nge-Muss-Liste.pdf> (besucht am 20. März 2019), 9;
Eine Übersicht der Blacklists der Datenschutzbehörden in der BRD findet sich unter: *Windelband*, Deutsche Aufsichtsbehörden legen Blacklist vor, vom 1. Juni 2018, erhältlich im Internet: <https://www.datenschutz-notizen.de/deutsche-aufsichtsbehoerden-legen-blacklist-vor-0920586/> (besucht am 01. März 2019).
[198] Einschränkend dazu bestehen Ausnahmen von dieser Pflicht gem. Art. 6 Abs. 1 DSGVO u. a. bei der Erfüllung öffentlicher Interessen sowie vertraglicher Verpflichtungen, *Gardyan-Eisenlohr/Cornelius*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 12, Rn. 75.
[199] *Oostveen*, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299 (308).

man zu diesem Sachverhalt die im vorherigen Kapitel geschilderte Problematik des Privacy Shield hinzu, kann ein Handlungsbedarf bei Unternehmen in diesem Bereich konstatiert werden.

Die angesprochene Problematik im Cloud-Computing kann analog auf diesen Bereich übertragen werden. Der Anwendungsbereich der DSGVO ist breiter, enthält tiefgreifendere Pflichten und im Falle eines Verstoßes hohe Strafen. Resultierend aus der Rechtsunsicherheit und wohlmöglich unzureichenden Reichweite von Privacy Shield kann empfohlen werden, die DSGVO-Konformität bei Unsicherheit über den Anwendungsbereich herzustellen, wenn personenbezogene Daten im Gesetzessinne in irgendeiner Form verarbeitet werden. Zusätzlich sollten Big-Data-Unternehmen die physischen Standorte ihrer Datenübermittlungen überprüfen.[200] Befinden diese sich in Drittländern wie den USA, sollt die Option der geeigneten Garantien geprüft werden, um nicht von einer eventuellen Ungültigkeitsentscheidung des EuGH überrascht zu werden.

III. E-Discovery

Am Bereich der sog. E-Discovery lässt sich beispielhaft illustrieren, wie die unterschiedlichen Rechtsregime kollidieren und dadurch bei Unternehmen und Betroffenen für Rechtsunsicherheit und Kosten sorgen könnten.

Das US-Prozessrecht, in diesem Fall die Federal Rules of Civil Procedure (FRCP), räumt jedem Kläger das Recht ein, von dem Beklagten vorgerichtlich die Offenlegung von Beweisen zu verlangen, die für die Begründung des Anspruchs gegenüber dem Beklagten nützlich sein könnten.[201] Ziel dieser Praxis ist es, das Verfahren vorgerichtlich abzukürzen.[202] Der Beibringungsgrundsatz i. V. m. dem Ausforschungsverbot verbietet dieses Vorgehen im europäischen Rechtsraum.[203]

Um solche internationalen Diskrepanzen bei grenzüberschreitender Beweiserhebung zu regulieren, wurde das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- und Handelssachen von 1970 entworfen. In diesem war ein bestimmtes Verfahren für die Beweisaufnahme vorgesehen. Unter anderem sollte bei der Beweisaufnahme das Datenschutzrecht der Vertragsparteien beachtet werden. Der US-Supreme Court urteilte jedoch hierzu, dass die Einhaltung des von den USA 1972 ratifizierten Abkommens für Kläger vor US-Gerichten nicht zwingend sei.[204] Als Folge ist ausländisches Datenschutzrecht in der E-Discovery in den USA nur unter bestimmten, engen Voraussetzungen zu beachten.[205]

[200] *Meyerdierks*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 132-136.
[201] *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (12); *Heinemann*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 81 ff.
[202] *Ibid*., Rn. 79.
[203] *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (12).
[204] *Ibid*., 12 f.
[205] *Ibid.*

Für transatlantisch operierende Unternehmen kann dies bedeuten, dass sie ihre Daten- und Informationssysteme der US-Gesetzgebung anpassen müssen, wollen sie Nachteile vor US-Gerichten vermeiden.[206] Wenn in einem solchen Verfahren jedoch personenbezogene Daten aus der EU betroffen sind, kollidiert das beschriebene US-Recht mit der DSGVO. Da das oben beschriebene US-Recht wiederum Grundlage für die Interpretation von Privacy Shield ist, sind Rechtskollisionen in diesem Bereich sehr wahrscheinlich. Dies soll an einem Beispiel illustriert werden.

Das beschriebene Auskunftsrecht für Kläger vor US-Gerichten betrifft alle Informationen, die nach Ansicht des Klägers für die Klage relevant sind. Also auch elektronische Dokumente wie E-Mails, die nicht unmittelbar Beweismittel sind, sondern mittelbar zum Beweismittel führen. Sobald ein Rechtstreit wahrscheinlich ist, verpflichtet der sog. „Legal hold" der FRCP, die Daten aufzubewahren. [207] Da das potentiell alle Daten eines Unternehmens betrifft, müssten betroffene Unternehmen ein sog. Evidence-and-discovery-management-System (EDRM) in ihre Geschäftsprozesse implementieren.[208] Das ist eine Software, die gemäß der E-Discovery-Vorgaben Beweise automatisiert sichert. Problematisch könnte sein, dass die Implementierung eines solchen Systems nicht nur Zeit und Geld kostet, sondern dessen Einführung und Durchführung der DSGVO in zentralen Bestandteilen widerspricht.[209]

Ein EDRM-System arbeitet dabei archetypisch in vier Phasen. Das sind die Identifikation, Sicherung, Bearbeitung und Übermittlung von potentiellen Beweisdaten.[210] Das Hauptaugenmerk wird des Umfangs dieser Abhandlung wegen auf der Übermittlung liegen.

Die Übermittlung von Beweisdaten fällt in den Anwendungsbereich der DSGVO, sofern es sich um personenbezogene Daten i. S. d. Gesetzes handelt. Analog zum Cloud-Computing und zu Big Data gelten für die aus US-Recht notwendige Übermittlung potentieller Beweise die Vorschriften für die Übermittlung solcher Daten in ein Drittland. Entsprechend sind Art. 44 und 45 DSGVO einschlägig.[211] Das heißt im ersten Schritt, dass es eines Erlaubnistatbestands gem. Art. 6 Abs. 1 DSGVO bedarf. Hierbei könnte besonders problematisch sein, dass die Übermittlung an US-Kläger nicht dem vorher definierten Zweck der ursprünglichen Erhebung entspricht und folglich rechtswidrig wäre.[212] Entsprechend wäre die erneute Einwilligung der ggf. betroffenen Personen unter Angabe des neuen Zwecks einzuholen.[213] Inwieweit dies z. B. bei Beschäftigungsdaten von Betroffenen mit dem ursprünglichen Zweck vereinbar sind, dementsprechend übermittelt werden dürften, ist umstritten. Im Zweifelsfall wird die Absprache mit dem Datenschutzbeauftragten empfohlen, um Strafen zu vermeiden.[214]

[206] *Ibid.*
[207] *Heinemann*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 83-86.
[208] *Ibid.*, Rn. 92 ff.
[209] *Ibid.*, Rn. 90.
[210] *Ibid.*, Rn. 96, 114.
[211] *Ibid.*, Rn. 114.
[212] *Ibid.*, Rn. 104; Erwägungsgrund Nr. 50 DSGVO.
[213] *Ibid.*, Rn. 107.
[214] *Ibid.*, Rn. 104.

Liegt wie zurzeit ein Angemessenheitsbeschluss mit der USA vor, unterliegen die Übermittlung vorbehaltlich des oben beschriebenen Erlaubnistatbestands keinem zusätzlichen Genehmigungsbedarf.[215] Die zweite Hürde wäre in diesem Fall genommen.

Strittig in diesem Zusammenhang ist jedoch die Reichweite des Art. 48 DSGVO. Dieser erlaubt Ersuchen und Urteile von US-Gerichten nach Übermittlung oder Offenlegung nur, sofern diese durch internationale Abkommen oder Rechtshilfeabkommen gedeckt sind.[216] Inwieweit Privacy Shield als Grundlage der Angemessenheitsentscheidung ein internationales Abkommen darstellt und damit hierfür ausreicht, ist fraglich.[217]

Zusätzlich bestehen innerhalb der EU unterschiedliche Rechtslagen. Die Bundesrepublik Deutschland hat dem Haager Übereinkommen von 1970 nur mit einem Vorbehalt gegenüber E-Discovery zugestimmt.[218] Im Endeffekt könnte dadurch nicht nur im transatlantischen, sondern auch im innereuropäischen Rechtsraum Potenzial für Rechtskollisionen bestehen.

Zusammengefasst kann konstatiert werden, dass die Rechtskonformität im Bereich Cloud-Computing, Big Data und E-Discovery im transatlantischen Verhältnis auf Privacy Shield fußt. Da dieses Abkommen aufgrund seiner fehlenden Reich- und Tragweite die Rechtsunsicherheit gemessen am neuen DSGVO-Maßstab fördert, wackelt dieses Fundament jedoch. Speziell die festgestellte Reichweite der DSGVO hat das Potenzial, Privacy Shield als Maßstab für Betroffene und Unternehmen *ad absurdum* zu führen.

Aus diesem Grund werden alternative, von der Angemessenheitsentscheidung und Privacy Shield unabhängige Rechtsgrundlagen für Datenübermittlungen in die USA oder andere Drittländer im nächsten Kapitel dargestellt und diskutiert.

E. Geeignete Garantien oder globale Lösung: Rechtliche Alternativen

I. Standard Contract Clauses

Die erste geeignete Garantie für Datenübermittlungen in die USA im Falle einer EuGH-Entscheidung gegen Privacy Shield sind die sog. Standard Contract Clauses (SCCs) gem. Art. 46 Abs. 2 lit. c) DSGVO. Dies sind von der EU-KOMM verfasste und aus der DSLR übernommene Standarddatenschutzklauseln. Unternehmen können diese verwenden und untereinander abschließen.[219] Sie würden ggf. den fehlenden

[215] Art. 45 Abs. 1 DSGVO.

[216] *Heinemann*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 17, Rn. 117.

[217] *Ibid*. Privacy Shield besteht aus Briefwechseln der zuständigen Behörden, einer Presseerklärung, den Datenschutzprinzipien, diese spezifizierenden Zusatzprinzipien und dem letztendlichen EU-KOMM-Beschluss. Ob dies für einen völkerrechtlichen Vertrag i. S. d. Art. 48 DSGVO ausreicht, wäre eine interessante Frage für zukünftige Analysen.

[218] *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (12).

[219] *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 159. Derzeit gibt es drei SCCs: Entscheidung der EU-KOMM Nr. 2001/497/EG, ABl. Nr. L 181/19 vom 15. Juni 2001, erhältlich im Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32001D0497&from=DE> (besucht am 9. Mai 2019),

oder für ungültig erklärten Angemessenheitsbeschluss kompensieren.[220] Des Weiteren sind sie nicht mehr von den Datenschutzbehörden gesondert genehmigungspflichtig, sobald sie erlassen wurden.[221] Ungeachtet dessen müssen die verantwortlichen Unternehmen die beschriebene DSGVO-Konformität der Datenübermittlungen im ersten Schritt nachweisen. Die nationalen Datenschutzbehörden können auch SCCs erlassen, haben allerdings aufgrund der Bewährtheit der bestehenden SCCs bis dato davon abgesehen.[222]

Der größte Nutzen der SCCs besteht in ihrer Praktikabilität. Analog zur Angemessenheitsentscheidung fällt eine kosten- und zeitaufwendige Genehmigung weg. Zusätzlich können die SCCs in bestehende Verträge zwischen Unternehmen integriert werden. Sie sind auch hier ressourcenschonend.[223]

Gleichzeitig stellt der europäische Gesetzgeber durch zwei Vorschriften für die SCCs sicher, dass das Datenschutzniveau der DSGVO gewährleistet wird.[224] Erstens gilt ein Änderungsverbot mit Genehmigungsvorbehalt. Wollen Unternehmen die Klauseln auf ihre individuellen Bedürfnisse anpassen, müssen die nationalen Datenschutzbehörden dies gem. Art. 46 Abs. 3 lit. a) DSGVO genehmigen. Entsprechend liegt hierin ein Nachteil der SCCs. Sie sind ihrem Wesen nach unflexibel.

Zweitens ist es für die Nutzung der SCCs Pflicht, dass der Datenexporteur sich in der EU befindet. Dadurch wird einerseits die Anwendbarkeit der DSGVO sichergestellt, weil die die in Kapitel C. III. beschriebenen Rechte von Betroffenen eingehalten werden müssen.[225] Andererseits könnte das Instrument sich durch diese einseitige Wirkrichtung seiner eigenen Wirksamkeit und Anwendbarkeit berauben. Eventuell könnten Unternehmen aber auch dazu gebracht werden, ihren Sitz nach Europa zu verlegen. Wird dieses Argument in den Kontext des extraterritorialen Anwendungsbereichs der DSGVO gestellt, ist die Relevanz des Unternehmenssitzes für die Anwendbarkeit der DSGVO jedoch nicht von Belang.

Für transatlantisch agierende Unternehmen auf der Suche nach einer ressourcensparenden, rechtssicheren aber nicht flexiblen Lösung sind SCCs entsprechend eine valide Lösung, sollte Privacy Shield der Überprüfung des EuGHs nicht standhalten. Betroffenenrechte werden durch die Standardisierung eingehalten und deren Durchsetzung ungeachtet des Marktortprinzips potenziell effektiver.

Entscheidung der EU-KOMM Nr. 2004/915/EG, ABl. Nr. L 385/74 vom 27. Dezember 2004, erhältlich im Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32004D0915&from=DE> (besucht am 9. Mai 2019) und Entscheidung der EU-KOMM Nr. 2010/87/EU, ABl. Nr. L 39/5 vom 5. Februar 2010, erhältlich im Internet: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32010D0087&from=DE> (besucht am 9. Mai 2019).

220 Art. 46 DSGVO.

221 *Moos/Zeiter*, in Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 49.

222 *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 159; das Verfahren für die Genehmigung nationaler SCCs regelt Art. 93 Abs. 2 DSGVO.

223 *Moos/Zeiter*, in Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 63-65.

224 *Ibid*., Rn. 63.

225 *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 63.

II. Binding Corporate Rules

Alternativ zu den SCCs können Unternehmen gem. Art. 46 Abs. 2 lit. b) DSGVO interne, verbindliche Datenschutzvorschriften erlassen. Dies sind die sog. Binding Corporate Rules (BCRs). Da die BCRs nur innerhalb von Unternehmen als geeignete Garantie für Drittlandsübermittlungen genutzt werden dürfen, eigenen sich diese nur für multinationale Unternehmensgruppen, insbesondere für europäische Cloud-Computing-Anbieter mit Niederlassungen in den USA.[226]

Im Gegensatz zu den SCCs dürfen BCRs auf die individuellen Bedürfnisse der Unternehmensstruktur angepasst werden. Sie sind gegenüber den SCCs entsprechend flexibel. Dafür unterliegen BCRs gem. Art. 47 Abs. 1 DSGVO einem individuellen Genehmigungsvorbehalt der Aufsichtsbehörden. Entsprechend wird die Flexibilität für Unternehmen mit zusätzlichen Kosten für das Genehmigungsverfahren aufgewogen.[227]

Das Genehmigungsverfahren selbst regelt Art. 63 DSGVO näher. Voraussetzung für die Genehmigung ist – analog zum Vorliegen eines Angemessenheitsbeschlusses oder einer SCC – ein Erlaubnistatbestand für die Datenübermittlung gem. Art. 6 Abs. 1 DSGVO. Im zweiten Schritt ist unter anderem die Beachtung der Mindestinhalte gem. Art. 47 Abs. 2 DSGVO für die Genehmigung ausschlaggebend, mit denen die einheitliche Wirksamkeit und effektive Reichweite der in Kapitel C. III. beschriebenen DSGVO garantiert werden soll.[228] Für Unternehmen und Betroffene besteht durch die BCRs eine Möglichkeit, Datenschutzrechte in Drittländern effektiv auszuüben oder wahrzunehmen. Wird die Genehmigung gem. Art. 63 DSGVO von der Aufsichtsbehörde in Absprache mit der EU-KOMM erteilt, gilt sie für alle erfassten Übermittlungen. Das Verfahren muss also nicht für einzelne Übermittlungen wiederholt werden. Es ist entsprechend für Cloud-Anbieter und Big-Data-Unternehmen eine Alternative.[229]

Zusammengefasst wären BCRs für Unternehmen mit Niederlassungen in den USA oder anderen Drittländern ohne Angemessenheitsbeschluss eine valide Alternative, um Rechtssicherheit zu garantieren. Voraussetzung dafür ist, dass das Unternehmen bereit ist, die größere Flexibilität des Mechanismus gegenüber der SCC zu erkaufen. Für die Übermittlung zwischen Unternehmen ist dieses Instrument allerdings nicht anwendbar und dessen Praktikabilität aus diesem Grund auf Konzernstrukturen reduziert.

III. Ausnahmeregelung im Einzelfall

Besteht kein Angemessenheitsbeschluss zwischen der EU und dem Drittland gem. Art. 45 Abs. 3 DSGVO und hat sich das Unternehmen keiner geeigneten Garantie gem. Art. 46 DSGVO unterworfen, ist der Datentransfer in ein Drittland gem.

[226] *Ibid.*, Rn. 68 ff.
[227] *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 70-74.
[228] *Ibid.,* Rn. 74 ff.; *Voigt/Von dem Busche*, EU-Datenschutz-Grundverordnung, 168 ff.
[229] *Ibid.*, Rn. 70.

Art. 49 DSGVO in bestimmten Fällen trotzdem zulässig.[230] Hierzu zählt u. a. die Einwilligung analog zu Art. 6 Abs. 1 lit. a) DSGVO, hier in Art. 49 Abs. 1 lit. a) aufgeführt, sowie alle anderen Erlaubnistatbestände des Art. 6 DSGVO.

Das Besondere an der Einwilligung ist, dass abseits der in Kapitel C. III. beschriebenen Informationspflichten zwei zusätzliche Pflichten bestehen. Der Betroffene muss über das Risiko eines Datentransfers in ein Drittland ohne Angemessenheitsbeschluss und geeignete Garantien aufgeklärt werden und muss dieser Übermittlung ausdrücklich zustimmen. Dieser Erlaubnistatbestand wird in der Praxis allerdings selten angewandt.[231]

Deutlich höhere Anwendung findet der Erlaubnistatbestand zur Erfüllung eines Vertrages gem. Art. 49 Abs. 1 lit. b). Dieser wird z. B. bei Reiseunternehmen zur Abrechnung von Hotels in Drittländern genutzt.[232]

Alle Ausnahmen des Art. 49 DSGVO gelten hierbei lediglich für Einzelübermittlungen. Für sich wiederholende Übermittlungen in Drittländer sind diese also für Big Data- oder Cloud-Computing-Anbieter im Gegensatz zu SCCs und BCRs nicht anwendbar und deswegen lediglich im Einzelfall praktikabel.[233]

IV. Regional Trade Agreements

Die bisher diskutierten Alternativen sind im Gegensatz zu Angemessenheitsbeschlüssen auf die Kooperation von einzelnen Unternehmen oder Unternehmensgruppen begrenzt. Jede Kooperation muss dabei einzeln verhandelt und im Fall der BCRs durch die Aufsichtsbehörden genehmigt werden. Abstrakt formuliert sind sie gegenüber einem Angemessenheitsbeschluss ineffizient, weil zusätzliche Transaktionskosten durch die Regelung auf der Individualebene entstehen.

Einerseits können Datenschutzrechte durch SCCs und BCRs abseits einer Angemessenheitsentscheidung in Drittländern vereinzelt garantiert und kontrolliert werden. Andererseits könnte dieser Standard auch durch Regulierung auf völkerrechtlicher Ebene in sog. Regional Trade Agreements (RTAs) erhalten oder sogar weiter durchgesetzt werden.[234]

Datenströme sind global und grenzüberschreitend. Zusätzlich haben viele Länder sehr geringen bis gar keinen kodifizierten Datenschutz.[235] Die völkerrechtliche Ebene in Form von RTAs könnte somit eine Möglichkeit darstellen, einen Mindeststandard

[230] *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 96 ff.
[231] *Moos/Zeiter*, in: Moos/Schefzig/Arning (Hrsg), Die neue Datenschutz-Grundverordnung, Kapitel 9, Rn. 97 f.
[232] *Ibid*., Rn. 104.
[233] *Ibid*., Rn. 114.
[234] *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (18).
[235] Dies gilt besonders für die Regionen Asien, Afrika, Russland und Südamerika, Welche Rolle spielt Datenschutz auf der Welt?, vom 30. Juni 2014, erhältlich im Internet: <https://www.haufe.de/compliance/recht-politik/laender-ranking-welche-rolle-spielt-der-datenschutz-auf-der-welt_230132_259132.html> (besucht am 19. März 2019).

an Datenschutz herzustellen. [236] Die zusätzlichen Transaktionskosten für Datenübermittlungen würden wegfallen. Gleichzeitig könnten Datenübermittlungen effizienter und sicherer werden.

Ein sog. Race to the bottom könnte hierdurch ebenfalls verhindert werden. In diesem nutzen Marktakteure schwache bzw. gar keine Datenschutzgesetze aus, um Daten von weniger geschützten Betroffen zu verarbeiten.[237]

Ob Freihandelsabkommen wie das aktuelle Japan-EU Free Trade Agreement (JEFTA) zwischen der EU und Japan in der Lage sind, Datenschutzstandards weiterzuentwickeln, kann kritisch betrachtet werden. JEFTA selbst enthält außer der in Kapitel C. I. angesprochenen Ausnahmeregelung des GATT bzw. GATS keine Datenschutzregelungen.[238]

Parallel zu den JEFTA-Verhandlungen wurden jedoch Verhandlungen zwischen der EU und Japan mit dem Ziel aufgenommen, den Datenschutz der beiden Wirtschaftszonen beiderseitig als angemessen zu erklären.[239] Japan sicherte im Zuge der Verhandlungen zu, seine Datenschutzgesetze anzupassen. So kam Japan u. a. der Forderung der EU einer unabhängigen und für Betroffene zugängigen Datenschutzbehörde nach. Die EU-KOMM hat darauf basierend ihren Angemessenheitsbeschluss für die Datenübermittlung zwischen Japan und der EU am 23. Januar 2019 erlassen.[240]

Beim auf *de facto* auf Eis liegenden Freihandelsabkommen Transatlantic Trade and Investment Partnership (TTIP) zwischen der EU und den USA wurde das Thema Datenschutz ebenfalls ausgeschlossen.[241] Ähnlich zum Angemessenheitsbeschluss von Japan wurde Privacy Shield parallel zu TTIP verhandelt.[242]

Die zwei Freihandelsabkommen wurden entsprechend weniger als materielle Alternative und mehr als Katalysator für parallele Verhandlungen zum Datenschutz genutzt. Dies könnte an der in Frage gestellten EU-Kompetenz liegen, gem. Art. 216 AEUV völkerrechtliche Verträge im Datenschutzbereich abzuschließen.[243]

Das Potenzial, Mindeststandards für Datenschutz in RTAs zu kodifizieren, wurde folglich noch nicht aktiviert. Im Sinne der Rechtssicherheit für Unternehmen und

[236] *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (18).

[237] *WTO*, World Trade Report 2018, 5.

[238] Art. 8.3 Abs. 2 lit. c) ii) des Freihandelsabkommens EU-Japan (JEFTA), vom 17. Juli 2018, 1 (194), erhältlich im Internet: <https://eur-lex.europa.eu/resource.html?uri=cellar:cf1c4c42-4321-11e8-a9f4-01aa75ed71a1.0003.02/DOC_2&format=PDF> (besucht am 7. März 2019).

[239] *EU-KOMM*, Europäische Union und Japan vereinbaren Schaffung des weltweit größten Raums für sicheren Datenverkehr, vom 17. Juli 2018, erhältlich im Internet: <http://europa.eu/rapid/press-release_IP-18-4501_de.htm> (besucht am 7. März 2019).

[240] *Ibid.*

[241] *Bendiek/Schmied*, SWP-Aktuell, Vol. 10 (2016), 1 (1).

[242] Dies geschah u. a. auch aus der Not der *Schrems*-Entscheidung heraus; vgl. dazu *Thüer*, EU-Innenausschuss zum Privacy Shield : Nachbessern oder aussetzen, vom 13. Juni 2018, erhältlich im Internet: <https://netzpolitik.org/2018/eu-innenausschuss-zum-privacy-shield-nachbessern-oder-aussetzen/> (besucht am 7. März 2019).

[243] *Weichert*, Datenschutz und Datensicherheit, Vol. 12 (2014), 850 (850); *Dix*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 5 (9); einschlägig für diese Debatte könnte die sog. Implied Powers-Lehre sein, vgl. dazu *Herdegen*, Europarecht, § 8, Rn. 71 ff.

Betroffene könnten RTAs auf langfristige Sicht jedoch eine echte Alternative darstellen, sofern die kompetenzielle Frage innerhalb der EU geklärt ist.[244]

Dies gilt umso mehr, da das GATS mit Art. XIV Regulierungen in RTAs Raum gibt. Inwieweit, wird im nächsten Kapitel diskutiert.

V. WTO-Reform: GATT und GATS als Mindeststandard

Im Kapitel C. I. wurde bereits die eventuelle Reformbedürftigkeit des WTO-Rechts in Form des GATT und des GATS bemerkt. Angesichts des globalen Datenhandels könnte die WTO mit ihren 164 Mitgliedern das richtige Forum sein, um Datenschutz und Datenhandel fernab der diskutierten Ausnahmeregelung in Art. XIV GATS zu regulieren. Dies sollte ursprünglich auch geschehen, scheiterte aber an den verschiedenen Positionen der Mitgliedsstaaten.[245] Stattdessen enthält der Entwurf des von 23 WTO-Mitgliedern verhandelten Trade in Services Agreement (TiSA) dem Artikel XIV GATS nachempfundene Vorschriften. [246] Die Verhandlungen liegen jedoch aktuell auf Eis.

In Verbindung mit dem vorausgegangenen Kapiteln könnte Art. XIV GATS in zukünftigen RTAs spezifiziert werden.[247] Datenschutzregeln könnten so auch in Wirtschaftszonen abseits Europas Einzug erhalten und vom europäischen zum globalen Standard werden. Nicht außer Acht zu lassen ist hierbei der Wettbewerbsvorteil durch Datenschutz für Unternehmen, der eventuelle Regulierungen fördern könnte.[248]

Dieser Gedanke muss jedoch mit Vorsicht betrachtet werden. Die europäische Idee eines Datenschutzgrundrechts lässt sich nur sehr begrenzt in einem ihr ideengeschichtlich verbundenen Staat wie der USA wiederfinden. Entsprechend schwierig könnten Verhandlungen um einen Mindeststandard mit 164 WTO-Mitgliedern sein, deren Vorstellungen von Datenschutz rechtshistorisch und soziokulturell anders gelagert sind. In diesem Kontext erscheint das Mittel der Ausnahme gem. Art. XIV GATS als kleinsten gemeinsamen Nenner als valide Möglichkeit, Datenschutz i. V. m. RTAs oder dem europäischen Weg der Angemessenheitsbeschlüsse multilateral zu fördern.

Das Fehlen eines völkerrechtlichen Mindeststandards als sog. Fall-back-Lösung könnte problematisch sein, wenn aus europäischer Sicht kein Mandat i. V. m. RTAs besteht und der Angemessenheitsbeschluss mit der USA wie beschrieben vom EuGH für unzureichend erklärt wird. Für Unternehmen und die Rechte von Betroffenen blieben in diesem Fall nur die dargestellten SCCs und BCRs als praktikable und rechtssichere Lösungen.

[244] Zum Inhalt von Privacy Shield vgl. *Weichert*, Privacy Shield, 5; zu Freihandelsabkommen als zukünftige Foren des Datenschutzes vgl. *Palmetshofer/Semsrott/Alberts*, Der Wert persönlicher Daten, Ist Datenhandel der bessere Datenschutz?, 33, vom Juni 2017, erhältlich im Internet: <https://bit.ly/2H3UhYu> (besucht am 18. März 2019).

[245] *Bendiek/Schmied*, SWP-Aktuell, Vol. 10 (2016), 1 (3 f.).

[246] *Ibid.;* Vgl. für den Stand der TISA-Verhandlungen *EU-KOMM*, Abkommen über den Handel mit Dienstleistungen (TiSA), vom 18. Juli 2017, erhältlich im Internet: <http://ec.europa.eu/trade/policy/in-focus/tisa/index_de.htm> (besucht am 8. März 2019).

[247] *Palmetshofer/Semsrott/Alberts*, Der Wert persönlicher Daten, Ist Datenhandel der bessere Datenschutz?, 33.

[248] *Ibid.*

Im abschließenden Fazit wird aus diesem Grund diskutiert werden, inwieweit die dargestellten Mechanismen Alternativen zum Privacy Shield darstellen.

F. Fazit: Rechts(un)sicherheit?

In der vorausgegangenen Analyse wurde das Privacy-Shield-Abkommen als Status quo im transatlantischen Datenschutz rekonstruiert. Dabei wurde das Abkommen zunächst in die derzeitige völkerrechtliche, amerikanische und europäische Rechtslage eingeordnet und anhand derer kritisch diskutiert.

Privacy Shield hat hierbei hinsichtlich unabhängiger Aufsichtsbehörden und der für EU-Bürger zur Verfügung stehenden Rechtsmittel Fortschritte erzielt. Gemessen an der weitreichenden DSGVO können diese jedoch als problematisch und deswegen unsicher eingestuft werden. Die im Außenministerium angesiedelte, damit nicht unabhängige und lange nicht besetzte Position der Ombudsperson für Datenschutzbeschwerden seitens der EU steht hierfür beispielhaft.

Hinzu kommt der bereichsspezifische, enge Anwendungsbereich des amerikanischen Datenschutzrechts. Dieser widerspricht dem allumfassenden Ansatz der DSGVO, grundsätzlich jede Datenverarbeitung zu erfassen und damit zu schützen. Da amerikanisches Recht aber Grundlage für die Interpretation von Privacy Shield ist, könnte der daraus resultierende, engere Schutzbereich bei einer Überprüfung des Angemessenheitsbeschlusses durch den EuGH problematisch werden. Ob der EuGH letztendlich Privacy Shield analog zum Vorgänger Safe Harbor für unzureichend und damit ungültig erklärt, vermag diese Analyse nicht final zu beurteilen. Jedoch bestehen aus den genannten Gründen berechtigte Zweifel an der Rechtssicherheit des Abkommens.

Daraufhin wurde die fehlende Praktikabilität des Privacy Shields festgestellt. Sobald Daten in irgendeiner Weise zwischen der EU und den USA übermittelt werden und personenbezogenen im Sinne der DSGVO sind, gilt die DSGVO. Transatlantisch tätige Cloud-Anbieter und Big-Data-Unternehmen müssen als Folge alle weitreichenderen Rechte und Pflichten der EU-Gesetzgebung einhalten. Dies gilt analog für Unternehmen, die ihre Daten im Zuge eines E-Discovery-Verfahrens in die USA übermitteln wollen. Bei Zuwiderhandlung drohen Verbandsstrafen in Höhe von 20 Mio. Euro bzw. 4 % des globalen Unternehmensumsatzes.[249] Im Ergebnis führt der extraterritoriale Anwendungsbereich der DSGVO die Vorschriften des Privacy Shields für transatlantisch tätige Unternehmen *ad absurdum*. Es lohnt sich für diese Akteure, DSGVO-konform zu sein. Zudem könnte robuster Datenschutz in Zukunft zum Marktvorteil werden. Der Nutzen einer angewandten DSGVO könnte im Verhältnis zu den Kosten also noch höher werden.

Im Sinne der Forschungshypothese kann zusammenfassend konstatiert werden, dass Privacy Shield aufgrund der dargestellten Ergebnisse den rechtlichen Anforderungen, insbesondere denen der DSGVO, hinterherhinkt. Unternehmen, die Privacy Shield als einzigen Maßstab ihrer Datenübermittlungen nehmen, riskieren die Rechtsgrundlage dieser. Ent-

[249] Art. 83 Abs. 5 lit. a) DSGVO.

sprechend birgt Privacy Shield nicht nur Risiken im Falle einer möglichen Ungültigkeitserklärung durch den EuGH im Allgemeinen, sondern auch im speziellen Verhältnis zu den weitreichenden Pflichten der DSGVO. Im Falle einer transatlantischen Tätigkeit kann als Empfehlung ausgesprochen werden, die DSGVO als Maxime des Handelns einzuführen, um Rechtsunsicherheit und Risiken zu vermeiden.

Einschränkend zu der Beantwortung muss jedoch bemerkt werden, dass Privacy Shield selbst eine Sonderstellung innehat. Lediglich vorbehaltlich der Zustimmung zu Privacy Shield gilt der Angemessenheitsbeschluss für die USA seitens der EU. In diesem Sinne ist Privacy Shield europarechtlich eine notwendige Bedingung, um den unsicheren und praktisch fragwürdigen Status quo aufrecht zu erhalten. Eine europarechtlich hinreichende Bedingung ist das Abkommen jedoch nicht.

Aus diesem Grund wurden in Kapitel E. alternative Rechtsgrundlagen für die Datenübermittlung diskutiert. Würde Privacy Shield nicht mehr gelten, stünden Unternehmen SCCs und Unternehmensgruppen BCRs als europarechtliche Alternativen zur Verfügung. Beide garantieren bei Anwendung zwar Rechtssicherheit, können aber nicht die Effizienz und Reichweite eines Angemessenheitsbeschlusses leisten. Die diskutierten Ausnahmeregelungen des Art. 49 DSGVO gelten ausdrücklich nicht für sich wiederholende Übermittlungen. Entsprechend sind sie für Unternehmen nicht praktikabel.

Die Analyse beschließend und vorausblickend konnte festgestellt werden, dass Datenschutz noch nicht oder sehr begrenzt in den globalen und regionalen Foren reguliert wird, in denen er längst hochrelevant geworden ist. Die Rechtswissenschaftlerin *Indra Spiecker gen. Döhmann* fasst die Relevanz dieser Problematik treffend zusammen.

> „Datenschutz ist kein national zu bewältigendes Problem mehr. Datenhandel findet weltweit statt, und viele Anbieter nehmen Datenverwendungen außerhalb Deutschlands und Europas wahr. An einem international gültigen Rechtsregime fehlt es indes, ebenso wie an Kollisionsregelungen, welche nationalen Regelungen im Konfliktfall anwendbar sein sollen."[250]

[250] *Spiecker gen. Döhmann*, in: Spiecker gen. Döhmann (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, 3 (3).

SCHRIFTTUM

Ad-Hoc EU-US Working Group on Data Protection, Report on the Findings of the EU Co-Chair of the Ad-Hoc EU-US Working Group on Data Protection, vom 27. November 2013, erhältlich im Internet: <https://bit.ly/2W6MAnd>(besucht am 18. März 2019).

Bender, David, Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield?, International Data Privacy Law, Vol. 6, Issue 2 (2016), 117-138.

Bendiek, Annegret/*Schmied*, Evita, EU-Außenhandel und Datenschutz: Wie lässt sich beides besser vereinbaren?, SWP-Aktuell, Vol. 10 (2016), Berlin 2016.

BITKOM, Cloud Computing – Evolution in der Technik, Revolution im Business, BITKOM-Leitfaden, Berlin 2009.

Brandt, Mathias, So viele Unternehmen zahlen für die Cloud, vom 01. September 2017, erhältlich im Internet: <https://de.statista.com/infografik/10923/cloud-computing-nutzung-von-unternehmen-in-deutschland/> (besucht am 26. Februar 2019).

Bremann, Nils, Öffnungsklauseln der DSGVO: Welche Gesetze gehen vor, vom 16. Februar 2018, erhältlich im Internet: <https://bit.ly/2TU3vMu> (besucht am 15. März 2019).

Cadwalladr, Carole/*Graham-Harrison,* Emma, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, vom 17. März 2018, erhältlich im Internet: <https://bit.ly/2plU1sM> (besucht am 1. Februar 2019).

Chaner, Apunam, Enabling and regulating the digital economy, in: WTO (Hrsg), World Trade Report 2018, The future of world trade: How digital technologies are transforming global commerce, Genf 2018, 194-195.

CNIL, The CNIL´s restricted committee imposes a financial penalty of 50 Million euros against Google LLC, vom 21. Januar 2019, erhältlich im Internet: <https://bit.ly/2FDztWt> (besucht am 18. Februar 2019).

Crain, Matthew, The limits of transparency, Data brokers and commodification, New Media & Society, Vol. 20, Issue 1 (2018), 88-104.

Culik, Nicolai, Brussels Calling: Big Data and Privacy, in: Hoeren, Thomas/Kolany-Raiser, Barbara (Hrsg), Big Data in Context, legal, Social and Technological Insights, Berlin 2018, 29-35.

Dix, Alexander, Datenschutz und transatlantische Freihandelszone, in: Spiecker gen. Döhmann, Indra (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, Karlsruhe 2013, 5-19.

EPRS, The Privacy Shield, Update on the state of play of the EU-US data transfer rules, vom Juli 2018, erhältlich im Internet: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf> (besucht am 19. März 2019).

EU-KOMM, Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, vom 19. Dezember 2018, erhältlich im Internet: <https://bit.ly/2BvTud2> (besucht am 18. März 2019).

– Europäische Union und Japan vereinbaren Schaffung des weltweit größten Raums für sicheren Datenverkehr, vom 17. Juli 2018, erhältlich im Internet:

<http://europa.eu/rapid/press-release_IP-18-4501_de.htm> (besucht am 7. März 2019).
– Abkommen über den Handel mit Dienstleistungen (TiSA), vom 18. Juli 2017, erhältlich im Internet: <http://ec.europa.eu/trade/policy/in-focus/tisa/index_de.htm>(besucht am 8. März 2019).

EU-Parliament, Committee on Civil Liberties, Justice Home Affairs, Background note on US legal Instruments for access and electronic surveillance of EU citizens, erhältlich im Internet: <https://bit.ly/2UHY8go> (besucht am 18. März 2019).

European Data Protection Supervisor, Opinion on the EU-U.S. Privacy Shield Adequacy Decision, Opinion No. 4 (2016), vom 30. Mai 2016, erhältlich im Internet: <https://bit.ly/2QqSSim> (besucht am 18. März 2019).

Gilbert, Francoise, EU General Data Protection Regulation: What Impact for Businesses Established Outside the EU, vom 19. April 2016, erhältlich im Internet: <https://bit.ly/2TT1hx0> (besucht am 14. Februar *2019).*

Herdegen, Matthias, Europarecht, 20. Aufl., München 2018.

Hessischer Datenschutzbeauftragter, Liste der Verarbeitungsmöglichkeiten nach Art. 35 Abs. 4 DS-GVO für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von durchzuführen ist, vom August 2018, erhältlich im Internet: <https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_Verarbeitungsvorg%C3%A4nge-Muss-Liste.pdf> (besucht am 20. März 2019).

Krempl, Stefan, Datenschutz: EU-Bürger erhalten theoretische Klagemöglichkeit in den USA, vom 25. Februar 2019, erhältlich im Internet: <https://www.heise.de/newsticker/meldung/Datenschutz-EU-Buerger-erhalten-theoretisch-Klagemoeglichkeit-in-den-USA-3117699.html> (besucht am 12. März 2019).

Lester, Simon/*Mercurio*, Bryan/*Davies,* Arwel, World Trade Law, Text, Materials and Commentary, 3rd ed., Oxford/London/New York/New Delhi/Sydney 2018.

Macaskill, Ewen/*Gabriel*, Dance, NSA Files: Decoded, What the revelations mean for you, vom 1. November 2013, erhältlich im Internet: <https://bit.ly/2dwNPcx> (besucht am 1. Februar 2019).

Mewes, Bernd, CLOUD Act – US-Gesetz für internationalen Datenzugriff und –schutz verarbschiedet, vom 24. März 2018, erhältlich im Internet: <https://www.heise.de/newsticker/meldung/CLOUD-Act-US-Gesetz-fuer-internationalen-Datenzugriff-und-schutz-verabschiedet-4003330.html?wt_mc=rss.ho.beitrag.atom> (besucht am 18. März 2019).

Moos, Flemming/*Schefzig*, Jens/*Arning*, Marian (Hrsg), Die neue Datenschutz-Grundverordnung, Berlin/Boston 2018.

Oostveen, Manon, Identifiability and the applicability of data protection on big data, International Data Privacy Law, Vol. 6, Issue 4 (2016), 299-309.

Palmetshofer, Walter/*Semsrott,* Arne/*Alberts*, Anna, Der wert persönlicher Daten, Ist Datenhandel der bessere Datenschutz?, vom Juni 2017, erhältlich im Internet: <https://bit.ly/2H3UhYu> (besucht am 18. März 2019).

Reding, Viviane, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, vom 22. Januar

2017, erhältlich im Internet: <http://europa.eu/rapid/press-release_SPEECH-12-26_de.htm> (besucht am 31. Januar 2019).

Roos, Ute, Westliche Länder haben beim Datenschutz die Nase vorn, vom 13. März 2014, erhältlich im Internet: <https://www.heise.de/ix/meldung/Westliche-Laender-haben-beim-Datenschutz-die-Nase-vorn-2169187.html> (besucht am 26. Februar 2019).

Schrems, Max, Privacy Shield – Press Breakfast with Jan Albrecht, vom 12. Juli 2016, erhältlich im Internet: <http://www.europe-v-facebook.org/PA_PS.pdf> (besucht am 18. März 2019).

Schulte, Laura, Vom quantitativen zum qualitativen Datenschutz, Leitbildwandel im Datenschutzrecht, Berlin 2018.

Schütz, Philip/*Karaboga*, Murat, Akteure, Interessanlage und Regulierungspraxis im Datenschutz, Eine politikwissenschaftliche Perspektive, Arbeitspapier des Forums Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe 2015.

Spiecker gen. Döhmann, Indra, Einleitung, in: Spiecker gen. Döhmann, Indra (Hrsg), Karlsruher Dialog zum Informationsrecht, Band 5, Karlsruhe 2013, 3-3.

Statista GmbH, Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung im Februar 2019, vom Februar 2019, erhältlich im Internet: <https://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/> (besucht am 18. März 2019).

– Anteil des Umsatzes von Amazon am gesamten Online-Handelsumsatz in Deutschland in den Jahren 2008 bis 2016, erhältlich im Internet: <https://de.statista.com/statistik/daten/studie/669851/umfrage/marktanteil-von-amazon-im-online-handel-in-deutschland/> (besucht am 18. März 2019).
– Marktanteile von Social Media Seiten nach Seitenabrufen weltweit von Dezember 2018 bis Februar 2019, erhältlich im Internet: <https://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit/> (besucht am 18. März 2019).

Thüer, Leo, EU-Innenausschuss zum Privacy Shield : Nachbessern oder aussetzen, vom 13. Juni 2018, erhältlich im Internet: <https://netzpolitik.org/2018/eu-innenausschuss-zum-privacy-shield-nachbessern-oder-aussetzen/> (besucht am 7. März 2019).

U.S. Department of Commerce, Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, erhältlich im Internet: <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g> (besucht am 21. Februar 2019).

– EU-US Privacy Shield Principles issued by the U.S. Department of Commerce, erhältlich im Internet: <https://bit.ly/2JkaKsR> (besucht am 18. März 2019).
– FAQs - General, erhältlich im Internet: <https://bit.ly/2FgOLxK> (besucht am 20. Februar 2019).
– Privacy Shield Framework, erhältlich im Internet: <https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text> (besucht am 25. März 2019).
– Privacy Shield List, erhältlich im Internet: <https://www.privacyshield.gov/list> (besucht am 19. Februar 2019).

U.S. Department of State, International Business Machines Cooperation, erhältlich im Internet: <https://www.privacyshield.gov/participant?id=a2zt0000000TOAoAAO&status=Active> (besucht am 26. Februar 2019).
– International Business Machines Cooperation, erhältlich im Internet: <https://www.privacyshield.gov/participant?id=a2zt0000000TOAoAAO&status=Active> (besucht am 26. Februar 2019).
– Privacy Shield Ombudsperson, erhältlich im Internet: <https://www.state.gov/e/privacyshield/ombud/> (besucht am 19. März 2019).
U.S. Senate Committee on Commerce, Science & Transportation, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, vom 18. Dezember 2013, erhältlich im Internet: <https://bit.ly/2W7VmkR> (besucht am 18. März 2019).
Voigt, Paul/*Von dem Busche*, Axel, EU-Datenschutz-Grundverordnung (DSGVO), Praktikerhandbuch unter vollständiger Berücksichtigung des deutschen Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU, Berlin 2018.
Voss, W. Gregory, The Future of Transatlantic Data Flows: Privacy Shield or bust, Journal of Internet Law, Vol. 19, No. 11 (2016), 1; 9-18.
Weichert, Thilo, Privacy Shield, Darstellung und rechtliche Bewertung, Kiel 2016.
– Freihandelsabkommen contra Datenschutz?, Datenschutz und Datensicherheit, Nr. 12 (2014), 850-856.
Weiss, Friedl, § 4 Internationaler Dienstleistungshandel, in: Tietje, Christian (Hrsg.), Internationales Wirtschaftsrecht, 2. Aufl., Berlin/Boston 2015, 237-268.
Weiss, Martin A./Archick, Kristin, U.S.-EU Privacy: From Safe Harbor to Privacy Shield, Congressional Research Report, No. R44257, vom 19. Mai 2016, erhältlich im Internet: <https://bit.ly/2PVPqt9> (besucht am 18. März 2019).
Wiegemann, Ann-Christin, Die Liberalisierung des Dienstleistungshandels im Recht der EU und WTO, Eine rechtsvergleichende Untersuchung, Baden-Baden 2009.
Windelband, Daniela, Deutsche Aufsichtsbehörden legen Blacklist vor, vom 1. Juni 2018, erhältlich im Internet: <https://www.datenschutz-notizen.de/deutsche-aufsichtsbehoerden-legen-blacklist-vor-0920586/> (besucht am 1. März 2019).
Wissenschaftlicher Dienst des Bundestages, Aktueller Begriff, Big Data, Nr. 37/13, Berlin 2013.
WP29, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, vom 13. April 2016, erhältlich im Internet: <https://bit.ly/2Fc2S7H> (besucht am 18. März 2019).
WTO, World Trade Report 2018, The future of world trade: How digital technologies are transforming global commerce, Genf 2018.
Zeni, Paola/*Gilbert,* Francoise/*Calehuff*, Max, GDPR and Privacy Shield: Different Tools for Different Goals, vom 26. November 2018, erhältlich im Internet: <https://www.francoisegilbert.com/?m=201811> (besucht am 21. Februar 2019).
Zwick, Detlev/*Dholakia*, Nikhilesh, Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right, Electronic Markets, Vol. 11, Issue 2 (2001), 116-120.

Beiträge zum Transnationalen Wirtschaftsrecht

(bis Heft 13 erschienen unter dem Titel: Arbeitspapiere aus dem Institut für Wirtschaftsrecht – ISSN 1619-5388)

ISSN 1612-1368 (print)
ISSN 1868-1778 (elektr.)

Bislang erschienene Hefte

Heft 100 Ernst-Joachim Mestmäcker, Die Wirtschaftsverfassung der EU im globalen Systemwettbewerb, März 2011, ISBN 978-3-86829-346-3

Heft 101 Daniel Scharf, Das Komitologieverfahren nach dem Vertrag von Lissabon – Neuerungen und Auswirkungen auf die Gemeinsame Handelspolitik, Dezember 2010, ISBN 978-3-86829-308-1

Heft 102 Matthias Böttcher, „Clearstream" – Die Fortschreibung der Essential Facilities-Doktrin im Europäischen Wettbewerbsrecht, Januar 2011, ISBN 978-3-86829-318-0

Heft 103 Dana Ruddigkeit, Die kartellrechtliche Beurteilung der Kopplungsgeschäfte von *eBay* und *PayPal*, Januar 2011, ISBN 978-3-86829-316-6

Heft 104 Christian Tietje, Bilaterale Investitionsschutzverträge zwischen EU-Mitgliedstaaten (Intra-EU-BITs) als Herausforderung im Mehrebenen-system des Rechts, Januar 2011, ISBN 978-3-86829-320-3

Heft 105 Jürgen Bering/Tillmann Rudolf Braun/Ralph Alexander Lorz/Stephan W. Schill/Christian J. Tams/Christian Tietje, General Public International Law and International Investment Law – A Research Sketch on Selected Issues –, März 2011, ISBN 978-3-86829-324-1

Heft 106 Christoph Benedict/Patrick Fiedler/Richard Happ/Stephan Hobe/Robert Hunter/Lutz Kniprath/Ulrich Klemm/Sabine Konrad/Patricia Nacimiento/Hartmut Paulsen/Markus Perkams/Marie Louise Seelig/Anke Sessler, The Determination of the Nationality of Investors under Investment Protection Treaties, März 2011, ISBN 978-3-86829-341-8

Heft 107 Christian Tietje, Global Information Law – Some Systemic Thoughts, April 2011, ISBN 978-3-86829-354-8

Heft 108 Claudia Koch, Incentives to Innovate in the Conflicting Area between EU Competition Law and Intellectual Property Protection – Investigation on the Microsoft Case, April 2011, ISBN 978-3-86829-356-2

Heft 109 Christian Tietje, Architektur der Weltfinanzordnung, Mai 2011, ISBN 978-3-86829-358-6

Heft 110 Kai Hennig, Der Schutz geistiger Eigentumsrechte durch internationales Investitionsschutzrecht, Mai 2011, ISBN 978-3-86829-362-3

Heft 111 Dana Ruddigkeit, Das Financial Stability Board in der internationalen Finanzarchitektur, Juni 2011, ISBN 978-3-86829-369-2

Heft 112 Beatriz Huarte Melgar/Karsten Nowrot/Wang Yuan, The 2011 Update of the OECD Guidelines for Multinational Enterprises: Balanced Outcome or an Opportunity Missed?, Juni 2011, ISBN 978-3-86829-380-7

Heft 113 Matthias Müller, Die Besteuerung von Stiftungen im nationalen und grenzüberschreitenden Sachverhalt, Juli 2011, ISBN 978-3-86829-385-2

Heft 114 Martina Franke, WTO, China – Raw Materials: Ein Beitrag zu fairem Rohstoffhandel?, November 2011, ISBN 978-3-86829-419-4

Heft 115 Tilman Michael Dralle, Der Fair and Equitable Treatment-Standard im Investitionsschutzrecht am Beispiel des Schiedsspruchs *Glamis Gold v. United States*, Dezember 2011, ISBN 978-3-86829-433-0

Heft 116 Steffen Herz, Emissionshandel im Luftverkehr: Zwischen EuGH-Entscheidung und völkerrechtlichen Gegenmaßnahmen?, Januar 2012, ISBN 978-3-86829-447-7

Heft 117 Maria Joswig, Die Geschichte der Kapitalverkehrskontrollen im IWF-Übereinkommen, Februar 2012, ISBN 978-3-86829-451-4

Heft 118 Christian Pitschas/Hannes Schloemann, WTO Compatibility of the EU Seal Regime: Why Public Morality is Enough (but May not Be Necessary) – The WTO Dispute Settlement Case "European Communities – Measures Prohibiting the Importation and Marketing of Seal Products", Mai 2012, ISBN 978-3-86829-484-2

Heft 119 Karl M. Meessen, Auf der Suche nach einem der Wirtschaft gemäßen Wirtschaftsrecht, Mai 2012, ISBN 978-3-86829-488-0

Heft 120 Christian Tietje, Individualrechte im Menschenrechts- und Investitionsschutzbereich – Kohärenz von Staaten- und Unternehmensverantwortung?, Juni 2012, ISBN 978-3-86829-495-8

Heft 121 Susen Bielesch, Problemschwerpunkte des Internationalen Insolvenzrechts unter besonderer Berücksichtigung der Durchsetzung eines transnationalen Eigentumsvorbehalts in der Insolvenz des Käufers, Juli 2012, ISBN 978-3-86829-500-9

Heft 122 Karsten Nowrot, Ein notwendiger „Blick über den Tellerrand": Zur Ausstrahlungswirkung der Menschenrechte im internationalen Investitionsrecht, August 2012, ISBN 978-3-86829-520-7

Heft 123 Henrike Landgraf, Das neue Komitologieverfahren der EU: Auswirkungen im EU-Antidumpingrecht, September 2012, ISBN 978-3-86829-518-4

Heft 124 Constantin Fabricius, Der Technische Regulierungsstandard für Finanzdienstleistungen – Eine kritische Würdigung unter besonderer Berücksichtigung des Art. 290 AEUV, Februar 2013, ISBN 978-3-86829-576-4

Heft 125 Johannes Rehahn, Regulierung von „Schattenbanken": Notwendigkeit und Inhalt, April 2013, ISBN 978-3-86829-587-0

Heft 126 Yuan Wang, Introduction and Comparison of Chinese Arbitration Institutions, Mai 2013, ISBN 978-3-86829-589-4

Heft 127 Eva Seydewitz, Die Betriebsaufspaltung im nationalen und internationalen Kontext – kritische Würdigung und Gestaltungsüberlegungen, August 2013, ISBN 978-3-86829-616-7

Heft 128 Karsten Nowrot, Bilaterale Rohstoffpartnerschaften: Betrachtungen zu einem neuen Steuerungsinstrument aus der Perspektive des Europa- und Völkerrechts, September 2013, ISBN 978-3-86829-626-6

Heft 129 Christian Tietje, Jürgen Bering, Tobias Zuber, Völker- und europarechtliche Zulässigkeit extraterritorialer Anknüpfung einer Finanztransaktionssteuer, März 2014, ISBN 978-3-86829-671-6

Heft 130 Stephan Madaus, Help for Europe's Zombie Banks? – Open Questions Regarding the Designated Use of the European Bank Resolution Regime, Juli 2014, ISBN 978-3-86829-700-3

Heft 131 Frank Zeugner, Das WTO Trade Facilitation-Übereinkommen vom 7. Dezember 2013: Hintergrund, Analyse und Einordnung in den Gesamtkontext der Trade Facilitation im internationalen Wirtschaftsrecht, Oktober 2014, ISBN 978-3-86829-735-5

Heft 132 Joachim Renzikowski, Strafvorschriften gegen Menschenhandel und Zwangsprostitution de lege lata und de lege ferenda, November 2014, ISBN 978-3-86829-739-3

Heft 133 Konrad Richter, Die Novellierung des InvStG unter besonderer Berücksichtigung des Verhältnisses zum Außensteuergesetz, März 2015, ISBN 978-3-86829-744-7

Heft 134 Simon René Barth, Regulierung des Derivatehandels nach MiFID II und MiFIR, April 2015, ISBN 978-3-86829-752-2

Heft 135 Johannes Ungerer, Das europäische IPR auf dem Weg zum Einheitsrecht Ausgewählte Fragen und Probleme, Mai 2015, ISBN 978-3-86829-754-6

Heft 136 Lina Lorenzoni Escobar, Sustainable Development and International Investment: A legal analysis of the EU's policy from FTAs to CETA, Juni 2015, ISBN 978-3-86829-762-1

Heft 137 Jona-Marie Winkler, Denial of Justice im internationalen Investitionsschutzrecht: Grundlagen und aktuelle Entwicklungen, September 2015, ISBN 978-3-86829-778-2

Heft 138 Andrej Lang, Der Europäische Gerichtshof und die Investor-Staat-Streitbeilegung in TTIP und CETA: Zwischen Konfrontation, Konstitutionalisierung und Zurückhaltung, Oktober 2015, ISBN 978-3-86829-790-4

Heft 139 Vinzenz Sacher, Freihandelsabkommen und WTO-Recht Der Peru-Agricultural Products Fall, Dezember 2015, ISBN 978-3-86829-814-7

Heft 140 Clemens Wackernagel, The Twilight of the BITs? EU Judicial Proceedings, the Consensual Termination of Intra-EU BITs and Why that Matters for International Law, Januar 2016, ISBN 978-3-86829-820-8

Heft 141 Christian Tietje/Andrej Lang, Community Interests in World Trade Law, Dezember 2016, ISBN 978-3-86829-874-1

Heft 142 Michelle Poller, Neuer Sanktionsrahmen bei Kapitalmarktdelikten nach dem aktuellen europäischen Marktmissbrauchsrecht - Europarechtskonformität des 1. FimanoG?, Januar

2017, ISBN 978-3-86829-876-5

Heft 143 Katja Gehne/Romulo Brillo, Stabilization Clauses in International Investment Law: Beyond Balancing and Fair and Equitable Treatment, März 2017, ISBN 978-3-86829-885-7

Heft 144 Kevin Crow/Lina Lorenzoni Escobar, International Corporate Obligations, Human Rights, and the Urbaser Standard: Breaking New Ground?, ISBN 978-3-86829-899-4

Heft 145 Philipp Stegmann, The Application of the Financial Responsibility Regulation in the Context of the Energy Charter Treaty – Case for Convergence or "Square Peg, Round Hole"?, September 2017, ISBN 978-3-86829-913-7

Heft 146 Vinzenz Sacher, Neuer Kurs im Umgang mit China? Die Reformvorschläge zum EU-Antidumpingrecht und ihre Vereinbarkeit mit WTO-Recht, Oktober 2017, ISBN 978-3-86829-918-2

Heft 147 Maike Schäfer, Die Rechtsstellung des Vereinigten Königreiches nach dem Brexit in der WTO: Verfahren, Rechtslage, Herausforderungen, November 2017, ISBN 978-3-86829-924-3

Heft 148 Miriam Elsholz, Die EU-Verordnung zu Konfliktmineralien Hat die EU die richtigen Schlüsse aus bestehenden Regulierungsansätzen gezogen?, Dezember 2017, ISBN 978-3-86829-926-7

Heft 149 Andreas Kastl, Brexit - Auswirkungen auf den Europäischen Pass für Banken, April 2018, ISBN 978-3-86829-936-6

Heft 150 Jona Marie Winkler, Das Verhältnis zwischen Investitionsschiedsgerichten und nationalen Gerichten: Vorläufiger Rechtsschutz und Emergency Arbitrator, April 2018, ISBN 978-3-86829-946-5

Heft 151 Hrabrin Bachev, Yixian Chen, Jasmin Hansohm, Farhat Jahan, Lina Lorenzoni Escobar, Andrii Mykhailov, Olga Yekimovskaya, Legal and Economic Challenges for Sustainable Food Security in the 21st Century, DAAD and IAMO Summer School, April 2018, ISBN (elektr.) 978-3-86829-948-9

Heft 152 Robin Misterek, Insiderrechtliche Fragen bei Unternehmensübernahmen Transaktionsbezogene Nutzung und Offenlegung von Insiderinformationen unter der Marktmissbrauchsverordnung, April 2018, ISBN 978-3-86829-949-6

Heft 153 Christian Tietje, Vinzenz Sacher, The New Anti-Dumping Methodology of the European Union – A Breach of WTO-Law?. Mai 2018, ISBN 978-3-86829-954-0

Heft 154 Aline Schäfer, Der Report of the Human Rights Council Advisory Committee on the activities of vulture funds and the impact on human rights (A/HRC/33/54): Hintergrund, Entwicklung, Rechtsrahmen sowie kritische völkerrechtliche Analyse, Juni 2018, ISBN 978-3-86829-957-1

Heft 155 Sabrina Birkner, Der Einwirkungserfolg bei der Marktmanipulation im Kontext nationalen und europäischen Rechts, Juli 2018, ISBN 978-3-86829-960-1

Heft 156 Andrej Lang, Die Autonomie des Unionsrechts und die Zukunft der Investor-Staat-Streitbeilegung in Europa nach Achmea, Zugleich ein Beitrag zur Dogmatik des Art. 351 AEUV, Juli 2018, ISBN 978-3-86829-962-5

Heft 157 Valentin Günther, Der Vorschlag der Europäischen Kommission für eine Verordnung zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Europäischen Union – Investitionskontrolle in der Union vor dem Hintergrund kompetenzrechtlicher Fragen, August 2018, ISBN 978-3-86829-965-6

Heft 158 Philipp Tamblé, Les dispositions sur le droit de la concurrence dans les accords d'intégration régionale, August 2018, ISBN 978-3-86829-967-0

Heft 159 Georgios Psaroudakis, Proportionality in the BRRD: Planning, Resolvability, Early Intervention, August 2018, ISBN 978-3-86829-969-4

Heft 160 Friedrich G. Biermann, Wissenszurechnung im Fall der Ad-hoc-Publizität nach Art. 17 MAR, März 2019, ISBN 978-3-86829-987-8

Heft 161 Leah Wetenkamp, IPR und Digitalisierung. Braucht das internationale Privatrecht ein Update?, April 2019, ISBN 978-3-86829-987-8

Heft 162 Johannes Scholz, Kryptowährungen – Zahlungsmittel, Spekulationsobjekt oder Nullum? Zivilrechtliche und aufsichtsrechtliche Einordnung sowie Bedürfnis und mögliche Ausgestaltung einer Regulierung, Mai 2019, ISBN 978-3-86829-996-0

Heft 163 Nicolaus Emmanuel Schubert, Aufschub von Ad-hoc-publizitätspflichtigen Informationen – Notwendigkeit, Probleme und Risiken, Mai 2019, ISBN 978-3-86829-998-4

Die Hefte 1 bis 99 erhalten Sie als kostenlosen Download unter:
http://telc.jura.uni-halle.de/de/forschungen-und-publikationen/beitr%C3%A4ge-transnationalen-wirtschaftsrecht